[The Complete] Management Solution
For Your Network

PRODUCT MANUAL

InocuLAN for NetWare
Supervisor's Guide

ManageWise™

MANAGEMENT SOFTWARE

Novell.

Credits   Written by Christopher B. Welch

Edited by Alex Chen, Victor Tsui, Thomas Mueller, Carl Oddo, Mark Lewis, Paul Nash, and Stone JyhKwei Shih

Product Support	If you have any questions about this product, please contact us at one of the following:

USA, Canada, Asia, Latin America: 3 Expressway Plaza Roslyn Heights, New York 11577 USA	Main Voice Number: Technical Support:	516-465-4000 800-CHEY-TEC Mon-Fri 8:00 am- 8:00 pm EST Mon-Fri 8:00 pm-10 pm EST (Callback only) Sat/Sun 10:00 am-4:00 pm EST (Callback only)
	Tech Support FAX: BBS: CompuServe: World-wide Web: FTP Server: InfoFax System:	516-465-5115 516-465-3900 GO CHEYENNE http://www.cheyenne.com/ ftp.cheyenne.com 516-465-5979 (Outside of North America you must use a fax machine's telephone.)
European Headquarters: Cheyenne Software S.A.R.L. Bel Air Building 58 rue Pottier 78150 Le Chesnay, France	Southern Europe Tech Support: Tech Support (FAX Hot Line): BBS: Infofax:	+33-1-49-93-90-34 Mon-Fri 09:00 - 17:00 +33-1-39-23-18-69 +33-1-39-23-18-60 +33-1-39-23-47-00
Germany: Cheyenne Software Deutschland Bayerwaldstr. 3 81737 Munich, Germany	Central and Eastern Europe Tech Support: Tech Support FAX: BBS (28800,N,8,1): BBS ISDN 64kB (v110, v120):	+49-69-920321-80 Mon-Fri 09:00 - 17:00 +49-89-627241-41 +49-89-627241-80 +49-89-627241-85
England: Cheyenne Software (UK) LTD Furness House 53 Brighton Road Redhill, Surrey, England RH1 6PZ	Northern Europe Tech Support: Tech Support FAX: BBS:	+44 (0) 990 239606 Mon-Fri 09:00 - 17:00 +44 (0) 990 785783 +44 (0) 990 143012
Japan: Cheyenne Software K.K. Sumitomo Fudosan Sanbancho Bldg. 3F, 6-26, Sanban-cho, Chiyoda-ku Tokyo 102, Japan	Voice: FAX:	+81-3-3222-3760 +81-3-3222-3762
Taiwan: Cheyenne Software, Taiwan Branch Room C, 4th Floor 170 Tun Hua North Road Taipei, Taiwan	Voice: FAX:	+886-2-545-5611 Mon-Fri 9 am- 5 pm +886-2-545-5616

Training	For the convenience of our customers, Cheyenne University has established a network of Authorized Cheyenne Education Centers and Authorized Cheyenne Instructors. For the latest course descriptions and schedules:

· Customers in U.S./Canada, call: 800-243-9272

· Customers in Europe, Africa, and Middle East, call: +33-1-39-23-18-80

· Customers in Australia, call +61-2-9591944

· Customers in Japan, call: +813-3222-3750

· Customers in Taiwan and Asia, call: +886-2-7951092

· Customers in other areas, call: +1-516-465-4000

C O N T E N T S

About InocuLAn

Scanning your Network with InocuLAN

Guarding your Network with InocuLAN

Alerting Users If a Virus is Detected

Command Line Operation

Using the InocuLAN Server

InocuLAN for DOS Basics

Scanning Your Network with InocuLAN for DOS

Guarding your Network

InocuLAN for Macintosh

Virus Recovery Procedures

Common Virus List

GETBBS.NLM

Installing InocuLAN Manager On the Client Desktop

1

C h a p t e r

ABOUT INOCULAN

InocuLAN AntiVirus for NetWare is an integrated client/server anti-virus solution for NetWare. It is designed to protect your file servers, workstations, and stand-alone computers from virus penetration.

In this chapter, you will learn:

Computer Viruses

A virus is a computer program that can destroy information on a file server or workstation. The three characteristics required in order to be classified as a virus are;

> ➤ executable file
> ➤ replicates itself
> ➤ attaches itself to other executables

Similar to a biological virus, a computer virus can reproduce itself by attaching to other files, usually executable programs. When isolated (non-executed, such as in a compressed file), computer viruses are not dangerous, but when they are accessed, they can create havoc.

How does your network get a virus?

Viruses are transmitted when an infected file is copied, downloaded, or used.

About 80% of viruses are transmitted by disk. Sometimes, off-the-shelf software contains viruses. If the virus is a "Boot Sector virus," it is spread when a workstation is booted up with the infected disk.

About 20% of viruses are transmitted by modem. Sometimes unsecured bulletin boards are the source of viruses and infected files are passed directly to a workstation or server.

Once an infected file finds its way to a server, the entire network can become infected.

How can you tell if
your computer has a
virus?

Symptoms of viral infection vary depending upon the particular virus infecting your system.   The following list contains some of the more common symptoms you are likely to encounter:

> ➣ Your screen displays a message such as "Your PC is now Stoned!".
> ➣ Your screen displays strange graphic patterns, such as bouncing balls.
> ➣ Files increase in size. Sometimes this is dramatic, causing the files to become too big to be loaded in memory. Frequently the change in size is small.
> ➣ The time stamp on a file is changed. You may notice a .COM or .EXE file with a time stamp more recent than when you loaded it.
> ➣ You get an error message about writing to a write-protected disk, even though your application is not attempting a write operation.
> ➣ It takes longer to load programs and your computer's configuration has not changed.
> ➣ Your computer seems to be running much slower than normal.
> ➣ Your computer has less memory available than normal.
> ➣ The same type of problems are occurring on several computers.
> ➣ You get a "Bad command or file name" error even when you know the file should be on the disk.
> ➣ You cannot access a drive that you know exists.

> ➢ CHKDSK suddenly discovers bad
>   sectors on more than one computer.
> ➢ You are having persistent problems on
>   one computer, such as difficulty in
>   copying files.
> ➢ Your computer locks up frequently.

If your computer exhibits one or more of these
symptoms, you may have a virus infection. Since it can
be difficult to determine if these symptoms are virus-
related, we suggest you use InocuLAN to confirm
whether or not your workstation or server is infected.

**What can a virus do
to your computer?**

Not all viruses damage your computer. Some viruses are
just nuisances, continually reproducing themselves or
displaying strange graphics and messages on your
screen.

Most viruses are stealthy, remaining hidden until they
start running.

If a virus does cause damage, the damage will vary
depending upon the particular virus infecting your
system. In general, viruses can do the following damage
to your computer:

> ➢ Hang your computer.
> ➢ Erase your files.
> ➢ Scramble data on your hard disk.
> ➢ Attack the File Allocation Table (FAT).
> ➢ Alter the partition table
> ➢ Format your hard disk.

Refer to Appendix A, "Common Virus List," for information about the damage specific viruses can cause.

Types of viruses

Viruses are classified according to how the virus is transmitted and how it infects the computer.

> **Boot Sector viruses** - These viruses overwrite the disk's original boot sector (which contains code that is executed when the system is booted) with its own code so that the virus is always loaded into memory before anything else. This means that every time you start your computer, the virus is run. Once in memory, the virus can make your startup disk unusable or can spread to other disks.

> **Master Boot Sector viruses** - These viruses overwrite the disk's master boot sector (partition table). These viruses are difficult to detect because many disk examination tools do not let you see the partition sector, which is the first sector on a hard disk.

> **Macro viruses** - These viruses are written in the macro language of specific computer programs, such as a word processor or spreadsheet. Macro viruses infect files (not the boot sector or partition table), and can become memory resident when executed. They can be run when a program document is accessed, or triggered by user actions, such as certain keystrokes or menu choices.

Macro viruses can be stored in files with any extension and are spread via file transfers, even over E-Mail.

➤ **File viruses** -These viruses infect other programs when an infected program is run. They do not remain in memory, so they do not infect the system. Like Memory Resident viruses (see below), non-resident viruses attach themselves to executable files. These viruses often change the file attribute information and the file size, time, and date information.

➤ **Multipartite viruses** - These viruses combine the characteristics of Memory Resident, File, and Boot Sector viruses.

Characteristics of viruses

The types of viruses listed above may exhibit different behavioral characteristics, based on how they function.

➤ **Memory Resident viruses** - These viruses load themselves in memory and take over control of the operating system. Memory Resident viruses attach themselves to executable files (such as .EXE, .COM, and .SYS files). These viruses often change the file attribute information and the file size, time, and date information.

➤ **Stealth viruses** - These viruses hide their presence. While all viruses try to conceal themselves in some way, Stealth viruses make a greater effort at concealment. For example, a stealth virus can infect a program, adding bytes to the infected file. It then subtracts the directory entry

of the infected file by the same number of bytes, giving the impression that the file's size has not changed.

➢ **Polymorphic viruses** - These viruses modify their appearance and change their signature (their identifiable code) periodically. For example, they may insert garbage code into the middle of a file execution, or change the order of execution. This allows the virus to escape signature scanning detection methods.

What is InocuLAN?

InocuLAN is an integrated client-server based anti-virus solution that provides network-wide protection for Novell NetWare local area networks (LANs). InocuLAN has three components:

> ➤ InocuLAN Server- installed with ManageWise 2.5 on a NetWare file server. (The server where InocuLAN Server is installed is called an InocuLAN domain server in this book.)
> ➤ InocuLAN Real Time Monitor - installed automatically on workstations at first login. Provides continual scanning of each workstation in the LAN.
> ➤ InocuLAN Manager - There are versions for Windows 3.x/Windows 95 as well as support for Macintosh workstations with InocuLAN for Macintosh.

InocuLAN protects against virus infection on all network nodes, including stand-alone and remote workstations, and NetWare 3.11, 3.12, and 4.x and up file servers.

Why do you need InocuLAN?

Computer viruses are an increasing problem for LANs. The cost of lost data and the time spent restoring infected file servers and workstations can be considerable if a virus infects your network.

Since file servers provide access to applications and information for all users on a network, one infected file on a server or workstation can spread quickly over the entire network. Therefore, it is critical that all servers and workstations remain virus-free.

How does InocuLAN work?

InocuLAN uses a client/server architecture to protect your network against virus infection. One client component of InocuLAN, the Real Time Monitor, runs on the workstation and is installed at login. The server component of InocuLAN installs with ManageWise 2.5 and runs on the server. The other client component, InocuLAN Manager, installs on the workstation.

Using a rules-based virus scanner to detect known viruses, InocuLAN scans DOS, Windows and Macintosh files on workstations and servers. In addition, InocuLAN offers real-time monitoring and a system integrity checker to protect workstations.

Extensive notification capabilities have been integrated into InocuLAN. MHS compliant E-mail, NetWare Global Messaging (NGM), alphanumeric pagers, FAX, Simple Network Management Protocol (SNMP), Trouble Tickets (print queue), and network broadcast messages are all available to make sure you are alerted when a virus is detected.

A sophisticated reporting mechanism records all InocuLAN operations, either client or server, in a centralized log.

In addition, if a virus is detected on the server you decide how the infected file should be handled. You can delete, rename, cure, move, report or purge an infected file. If InocuLAN Manager has been installed on the workstation, the user can handle infection at the desktop.

Virus Prevention Methods

There are four techniques that InocuLAN for Netware uses to detect computer viruses:

➢ Integrity Checking- determines if the program's file size has increased due to a virus attaching itself to a program. InocuLAN uses integrity checking primarily to check the integrity of the Critical Disk Area information.

➢ Rules-based Detection- observes the way programs behave to detect suspicious program behavior.

➢ Interrupt Monitoring- observes all program system calls (i.e. DOS and Macintosh) in an attempt to stop the sequence of calls which may indicate virus actions.

➢ Signature Scanning- uses a unique set of hexadecimal code, the virus signature, which a virus leaves within an infected file. By searching the program files armed with these codes, the signature scanner can detect that known virus.

InocuLAN
Architecture

To help you manage InocuLAN on your multi-server network, InocuLAN uses a concept called "domains." A domain is a group of one or more InocuLAN servers that can share configuration information and resources. Within a domain you only have to enter configuration information once. The master server downloads the information to all of its members and uploads information about activities on each member server, such as scanning messages. In addition, you can scan all of your domain members by setting up one scan.

InocuLAN Features

This release of InocuLAN contains many new features and enhancements, including the following:

➤ **Full NetWare NDS compatibility** lets you take advantage of the latest network operating system functionality.

➤ **Universal login allows** the administrator to login to the proper InocuLAN server to administrate all servers with a single login process.

➤ **Powerful new state-of-the-art detection technology** provides unmatched virus protection.

➤ **Completely redesigned, highly intuitive interface** incorporates the ease of a tree view browser with new detail volume information and versatile Point-to-Point network management.

➤ **Streamlined and simplified** new one-step installation program allows you to install both server and workstation components at the same time.

➤ **Scanning of compressed files,** such as ZIP files, is now available.

➤ **Critical Disk Area backup** now saves AUTOEXEC.BAT and CONFIG.SYS information, as requested by users.

➤ **Windows Real-time monitor** is now a separate VxD (Virtual Device Driver) program, not a DOS TSR.

➤ **Workstation scanning records** can now be viewed from the Domain Manager.

➣ **Server update program (SUPDATE) enhanced** to provide unattended server updating. Multiple servers can be set up in SUPDATE and then launched at one time. SUPDATE will now also automatically unload and reload the appropriate files on the server.

➣ **Reduced conventional memory requirement** for the DOS Manager compared to the previous release.

➣ **New and enhanced** documentation and on-line help.

➣ **Enforcement** can now be set using workstation addresses, as well as users and groups.

➣ **Customized Warning Messages** allows personalized alert messages to display when an virus intrusion occurs.

The following standard features continue to make InocuLAN the intelligent anti-virus software choice. You can specify exactly how you want these features to work for you.

➣ **Real-time monitor** scans all files as they enter or exit NetWare 3.11, 3.12, and 4.x file servers so that InocuLAN can ensure around-the-clock anti-virus security.

➣ **Scheduled Scanning** with maximum CPU utilization setting allows administrators to perform immediate or interval server scanning and set limits for CPU utilization. This prevents scanning from affecting server and network performance.

➤ **Auto-Download and File Synchronization** automatically distribute software upgrades and virus signature updates among file servers and workstations. Modem-equipped servers can be designated to automatically download the latest signature file from Cheyenne's BBS. This ensures the most current virus defense.

➤ **Domain Support** allows your InocuLAN servers to share configuration information. This centralizes and eases management of multiple server environments.

➤ **Alert System** immediately notifies selected users of a virus threat through network broadcast, print queue/trouble ticket, NGM, MHS E-mail, SNMP, FAXserve, and alphanumeric pager. This helps to quickly contain the virus spread.

➤ **Flexible Reporting** includes server scanning results, client virus incidents, configuration changes, and status reports. Reports are completely automated and fully support domains.

➤ **Windows, DOS, and Macintosh Client Support** provides all Novell networked and non-networked workstations with full InocuLAN functionality, including protection against file and boot viruses, multipartite, stealth, and polymorphic viruses, as well as virus-like activity. This helps safeguard your heterogeneous environment (including isolated machines) from known and unknown virus threats.

➤ **WIMMUNE** program detects known viruses and unknown viruses (viral behavior), scans files as they are about to be executed or opened, and examines memory for viruses. For DOS users, the IMMUNE TSR performs the same functions.

➤ **Enforcement** ensures that all workstations have the WIMMUNE program or IMMUNE TSR loaded before they can log in to a server. If the workstation does not have one of these loaded, the user will be denied entry to the server and the administrator will be notified. This option enhances security, keeping the environment virus-free.

➤ **Critical Disk Area protection** checks the CMOS RAM information, master boot sector, operating system boot sector, partition table, I/O system file, and other critical system files for viruses and/or viral damage. This critical area is backed up by InocuLAN, examined, and can be restored upon infection or corruption.

➤ **Command Line Support** allows InocuLAN to be initiated through robust command line operations, offering transparent operations to the end user.

About This Manual

The purpose of this manual

The goal of this manual is to show you how to use InocuLAN AntiVirus for NetWare, as implemented for ManageWise 2.5. Most of the information in this manual applies to Inoculan AntiVirus in general, as modifications required at installation and other configuration issues in this manual are now handled automatically in the ManageWise installation process.

What's in this manual?

This manual is divided into eight sections. Overall, there are 11 chapters and three appendices in this manual. The sections and chapters are listed below:

Overview of Chapters

➢ **Chapter 1: About InocuLAN** - Provides an overview of InocuLAN and this manual.

➢ **Chapter 2: Scanning your Network with InocuLAN** - Explains how to scan workstations and file servers for viruses with InocuLAN for Windows.

➢ **Chapter 3: Guarding your Network with InocuLAN for Windows** - Describes how to protect your network from viruses using InocuLAN for Windows.

Alert

➢ **Chapter 4: Alerting Users If a Virus is Detected** - Prepares InocuLAN to send NetWare broadcasts, electronic mail, FAX, SNMP, and pager notification.

Command Line/ Server Operation

➢ **Chapter 5: Command Line Operation** - Explains how to run InocuLAN from the command line.

➣ **Chapter 6: Loading and Using the InocuLAN Server** - Explains how to start and use the InocuLAN Server.

InocuLAN for DOS

➣ **Chapter 7: InocuLAN Basics** - Explains how to start InocuLAN for DOS and how to use common InocuLAN for DOS functions.

➣ **Chapter 8: Scanning your Network with InocuLAN for DOS** - Explains how to scan workstations and file servers for viruses.

➣ **Chapter 9: Safeguarding your Network with InocuLAN for DOS** - Describes how to protect your network from viruses.

InocuLAN for Macintosh

➣ **Chapter 10: Installing and using InocuLAN for Macintosh** - Explains how to install and use InocuLAN for Macintosh to protect your Macintosh workstation.

Recovering from a virus

➣ **Chapter 11: Virus Recovery Procedures -** Explains how to recover from a virus.

Appendices

➣ **Appendix A** - Lists common computer viruses.

➣ **Appendix B** - Describes how to configure and use GETBBS.NLM.

➣ **Appendix C** - Describes the procedure to install the full InocuLAN program on Windows 95 and 3.x workstations.

2

C h a p t e r

SCANNING YOUR NETWORK WITH INOCULAN

InocuLAN has several scanning options that you can use to scan your network in order to keep it virus free.

In this chapter, you will learn:

Selecting a Scanner

There are two scanning options you can use to scan your network from the InocuLAN Console:

➢ Domain Manager
➢ Local Scanner

You can also initiate a scan of a domain server directly from the server console.

If you want to scan a Macintosh workstation, you can use InocuLAN for Macintosh. Refer to Chapter 10 for more information.

Domain Manager

The Domain Manager lets you administer scanning jobs on all of your domain servers. You can run the scan immediately or schedule it to start at a later time. Scanning can be repeated at regular intervals. This function is only available for supervisors or supervisor equivalents.

> **NOTE: To learn more about domains, or for instructions on how to set up a domain, see chapter 3.**

Local Scanner

The Local Scanner option scans files on a local workstation or a mapped drive. The server does not have to be an InocuLAN domain server.

Selecting the correct scanner

If you cannot decide which scanner you need to use, refer to the following table. This table summarizes the basic functions of each scanner:

	What is scanned	File types	Who can use this scanner	Scanning occurs
Submitted by Domain Manager	InocuLAN domain server volumes	DOS, Windows and Mac	Supervisor or equivalent	Immediate, scheduled, or repeated at periodic intervals
Executed by Local Scanner	Any server*, local workstation, or floppy diskette	DOS and Windows	User or Supervisor	Immediate

NOTE: You cannot use this option for a server that has real-time scanning enabled. Viruses will be reported by the Real-time Monitor.

Using the Domain Manager

The Domain Manager can scan files on all domain member servers or on an individual member. The scanning can be scheduled or it can be run immediately. Scanning can be repeated at varying intervals. The actual scanning is done by InocuLAN's NLM on the server.

You can scan all of your domain members by setting up one scan job. The information for the scanning job will be propagated to all of your domain members. For example, by setting up a job to scan the SYS volume on your master server, you will scan the SYS volume on all of your domain member servers.

With the new Tree View Browser, you can have updated information of the various InocuLAN server readily available with automated update intervals and detail server information. You can even connect to a remote server with the new Point-to-Point Direct Connection functions.

The new Domain Manager also allows you to manually refresh the Tree View Browser, or configure it to automatically update the network tree information at a specific interval. To set the automatic refresh interval, you must select the _Domain_ command at the menu bar,

then the *Refresh* option, and the *Change Refresh Interval* command. This will bring up the Change Refresh Interval menu:
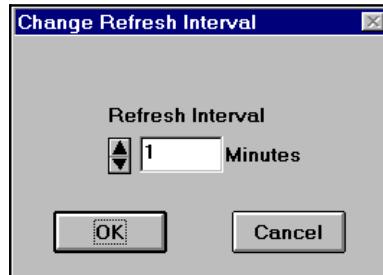
Instructions for a basic scan

Follow the instructions below to perform a basic scan of a domain using the Domain Manager. Information about using available scanning actions and options begins on page on page 2-10.

1. Click the Domain button.

The Domain Manager screen appears:

Click on this button to modify
the InocuLAN Domain.
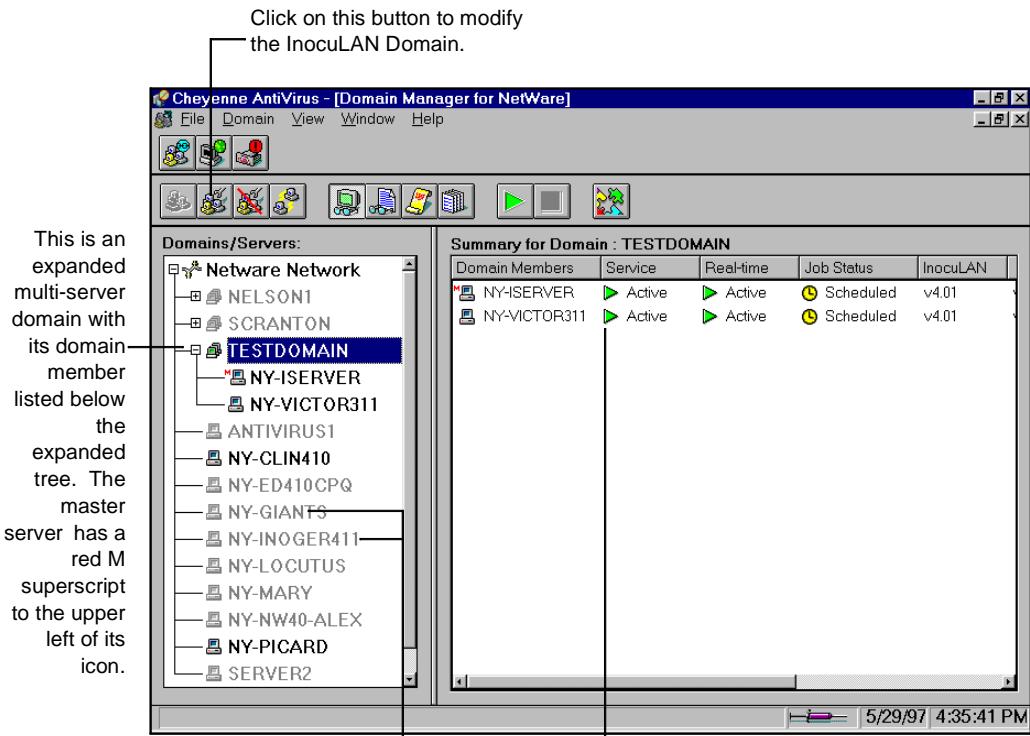
This is an
expanded
multi-server
domain with
its domain
member
listed below
the
expanded
tree. The
master
server has a
red M
superscript
to the upper
left of its
icon.

These grayed server listing does not have InocuLAN
installed thus they are not available to the Domain
Manager.

This screen displays the
domain members and its
service status.

The symbols in the Domains/Servers window are
explained below:

2. Highlight a domain.

3. Click the Add/Re-Schedule a Scan Job button.

	=	Master Server	The Master Server controls the members of its domain.
	=	Expandable Domain	Double-click to see all of the member machines of this domain.
	=	Expanded Domain	Click to collapse this domain.
	=	Single Server	This server is available to include in a domain.
	=	Orphan Domain	This domain was deleted. The master is now part of a new domain. This is not a normal condition. Delete the orphan domain and create a new domain.

This button starts or schedules a job. The Job Properties window appears:
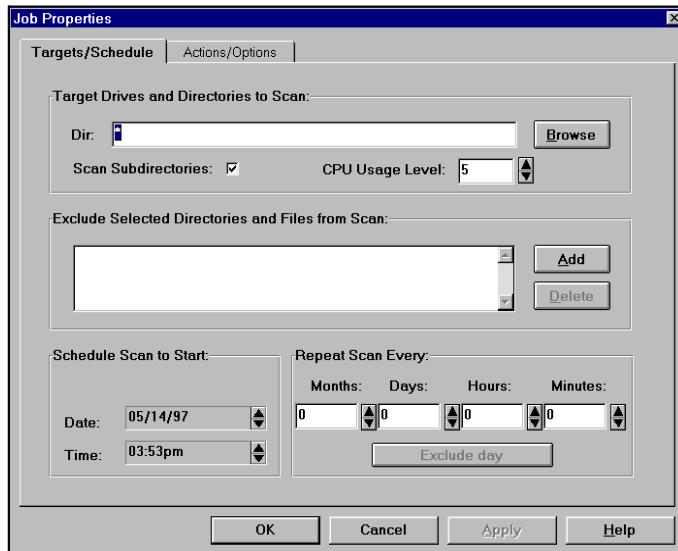
4. Enter information on the Schedule New Scan Job screen.

Target Drives and Directories to Scan	Enter the target drives, directories or volumes to scan. You can browse by clicking the Browse button.

> **NOTE: In the Dir: field, an asterisk (*) means InocuLAN will scan all of the volumes on the domain members. It will not scan floppy drives or mapped drives.**

Scan Subdirectories	Check to scan all subdirectories beneath the scan source.
CPU Usage level	Enter a value from 1-99 percent. This allows you to adjust the maximum level of CPU utilization when running the Domain Manager. For example, if you set the field to 35 percent, InocuLAN scanning will slow down if CPU utilization surpasses 35 percent.
Exclude Selected Directories and Files from Scan	You can exclude specific files or directories from being scanned. For example, you might want to exclude all files in a directory used for research purposes only.
	To specify a file or directory, click Add. Type in the name of the file or directory and click OK. Since a file or directory may not exist on every machine, InocuLAN will only apply the exclusion to those machines that contain the file or directory you specified.
Schedule Scan to Start	Indicate when the scan should run. The default is the current date and time.
Repeat Scan Every	If you want the scan to take place a single time, these fields should be left at zero.

If you want the scan to run at regular intervals, specify the time interval between each scan.

If you wish to exclude a particular day or days of the week from the scanning schedule, click the Exclude Day button. In the Exclude Day window, you can select one or more days on which a scheduled scan will *not* be run.

The Exclude Day button will only be active if at least one of the *Repeat Scan* fields is set to 1 or greater.

5. Click OK when done.

Point-to-Point network management.

To connect with the Point-to-Point Connection feature, you must first launch the Domain Scanner program. Then click on the Create a direct connection to an active server icon. A dialog box titled Select InocuLAN NetWare Server will appear. Select the specific NetWare server by the server's name and click OK.

After the direct connection has been made, you can administrate the active InocuLAN server by expanding the Tree View Browser under the Direct Connections branch.

Actions and Options for Domain Scans

InocuLAN provides a host of actions and options to customize the scanning process, including selecting file types to scan, the action to take if a virus is found, and skipping or including certain kinds of files.

InocuLAN's scanning Actions

To apply an action:

1. Click the Actions/Options tab on the Job Properties screen.
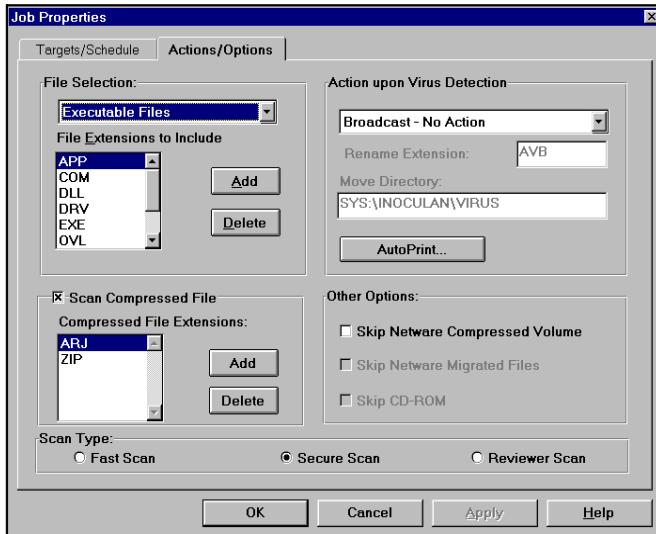
2. Select the actions you want to include with the scanning job.

DOS File Selection

You can select all files or a selection of executable files. If you select *Executable Files*, you can further define which files to scan by their extensions.

Click the Add button to enter an executable file type.

To delete a file type from the list, highlight it and click Delete.

Action upon Virus
Detection

Select one of the options described below. Regardless of which option you choose, a message will be broadcast when a virus is detected.

NOTE: **InocuLAN's Alert system can be configured to send a message to people in your organization when a virus is encountered. Messages can be sent via pager, e-Mail, FAX, NetWare broadcast, SNMP, or trouble-tickets sent to a printer. This assures that any viral infection on your network is immediately communicated to the people responsible for taking corrective actions. To configure the Alert service, refer to Chapter 4, "Alerting Users If a Virus is Detected."**

Action	Description
Report Only - No Action	Sends messages to Alert via Broadcast, Fax, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Report Log.
Delete File	Deletes an infected file from the machine.
Rename File	Renames infected files by giving them an .AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners.
	If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.

Action	Description
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to 'Rename File' below). <u>Even if InocuLAN cures the file, we recommend you purge the infected file and then restore the original file</u>.
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory.
Purge File	Deletes an infected file so that it cannot be recovered (for example, using Novell's Salvage utility).
Rename and Move File	Renames infected files by giving them a different extension and then moves them to the INOCULAN\VIRUS directory.
Copy and Cure File	Will make a copy of the infected file to the INOCULAN\VIRUS directory and continues to cure the file.

NOTE: If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

AutoPrint

Select AutoPrint to automatically print the results of the job scan. When you click the AutoPrint button, the following screen appears:

```
┌─────────────────────────────────────────────────┐
│ ─│              Print Options                    │
├─────────────────────────────────────────────────┤
│ ☒ AutoPrint Scan Job Scan Log Report            │
│ ┌─Printer Queue:─────────────────────────────┐  │
│ │                                            │  │
│ │  Server:    │NY-WRITER            │    ▼│  │
│ │                                            │  │
│ │  Name:      │PETER                │       │  │
│ │                                            │  │
│ │  Password:  │*****                │       │  │
│ │                                            │  │
│ │  Queue:     │LJ4                  │       │  │
│ │                                            │  │
│ └────────────────────────────────────────────┘  │
│                                                 │
│        ┌────────┐  ┌────────┐  ┌────────┐       │
│        │   OK   │  │ Cancel │  │  Help  │       │
│        └────────┘  └────────┘  └────────┘       │
└─────────────────────────────────────────────────┘
```
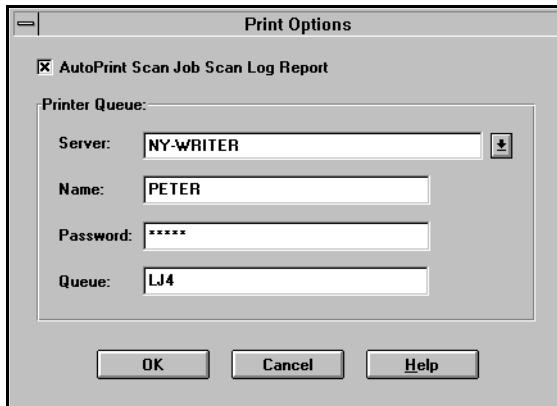
Select a server using the drop-down list, then enter your user name and server password.

In the Queue field, enter your NetWare printer queue name. If you do not know your printer queue name, open the DOS prompt window, type PCONSOLE at the command line, and press Enter to access the NetWare Print Console. Select Print Queue Information from the menu to see your print queue choices. Press ESC to exit the Print Console and return to the DOS prompt.

For an NDS queue, you must provide a distinguished (complete) name.

If you need additional instructions on how to use the Print Console, consult your NetWare administrator.

3. Click OK to set your Action selections, or click the Options tab to set scanning options.

To set InocuLAN's scanning options:

1. Click the Actions/Options tab on the Job Properties screen.

Job Properties
Targets/Schedule	Actions/Options

File Selection:

Executable Files

File Extensions to Include

APP
COM
DLL
DRV
EXE
OVL

Add

Delete

Action upon Virus Detection

Broadcast - No Action

Rename Extension: AVB

Move Directory:
SYS:\INOCULAN\VIRUS

AutoPrint...

☒ Scan Compressed File
Compressed File Extensions:

ARJ
ZIP

Add

Delete

Other Options:

☐ Skip Netware Compressed Volume

☐ Skip Netware Migrated Files

☐ Skip CD-ROM

Scan Type:
○ Fast Scan   ● Secure Scan   ○ Reviewer Scan

OK   Cancel   Apply   Help

2. Select the options you want to include with the scanning job.

Choose one of the following scanning options:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.

Scan Type	Description
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Skip Netware Compressed Volume

This option will cause InocuLAN to avoid scanning any NetWare compressed files on your servers. This is the default value. Scanning compressed files will increase the scanning time.

Skip Netware Migrated Files

The function is reserved for future use and is not available at this time.

Skip CD-ROM

This function is reserved for future use and is not available at this time.

Scan Compressed Files

Select this option for InocuLAN to scan compressed files. By default, InocuLAN scans files of the ZIP and ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, click the Add button.

3. Click OK when done.

Modifying a Scan Job

Once you have scheduled a new scan job, it can be modified to fit your requirements.

1. In the Domain Manager, click the Scan Job and Log View button.

   Highlight the scheduled job in the Job Queue Screen.

2. Click the Add/Re-Schedule a New Scan Job button, or double click on the specific scan job in the job queue.

3. The Add or Re-Schedule a Scan Job menu will display:

Add or Re-Schedule a Scan Job
Add New Scan Job
Re-Schedule the Selected Scan Job
Cancel
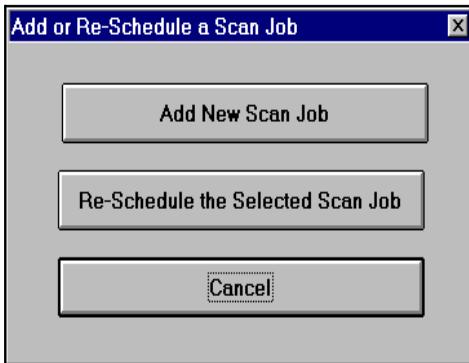
Select an option.

4. The Job Properties screen is displayed once more:
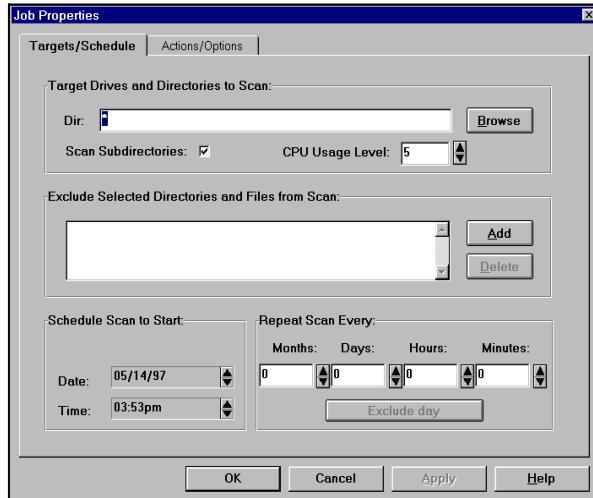
5. Make the changes in either the Job Properties screen, and the Actions/Options screen.

6. Click OK when done to resubmit the scan job.

Checking the Progress of Your Scan Job

You can view the steps of your scan while it is in progress.

1. In the Domain Manager, click the Scan Job and Log View button.

   The Scan Job Queue screen appears:

The scheduled scan job is displayed in the Job Queue window.

2. Double-click on the active job.

   The Job Scan Progress screen appears:

Screen information is updated as the scan continues. The status bar at the bottom of the window shows what percentage of files have been

Job Scan Progress

Job Information:

Target Server:	NY-SUNNY
Target Dir(s):	SYS:, Subdirectories Included.
Job Status:	Scanning

Scanning File:

SYS:\ACCESS\INSTALL\SETUP.EXE

Job Statistics:

# Dirs:	60	# Infected:	0
# Files:	126	# Viruses:	0
KBytes:	10721		
% Done:		92%	
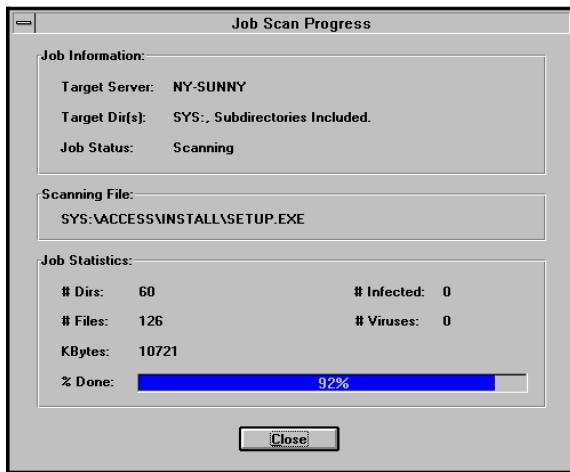
[Close]

3.   Click Close when done.

Checking the Results of Your Scan Job

Follow the instructions below to see the results of the Domain Scan:

1. Highlight a domain.

2. Click the Scan Job and Log View button.

    The screen displays the results of all Domain scanning jobs.

3. Double-click on a log in the Job Log Report window to view job details.

This screen displays detailed information about the scanning job.

```
┌─────────────────────────────────────────────────────────────────┐
│ ─ │                    View Record #4                            │
├─────────────────────────────────────────────────────────────────┤
│ ┌─────────────────────────────────────────────────────────────┐▲│
│ │              ServerName : NY-SUNNY                           │ │
│ │ 09/19/95 16:13 Start SCHEDULED SCAN.   Volume - SYS:         │ │
│ │ 09/19/95 16:13 Executable Dos Files to be Checked: *.APP *.COM *.DLL *.DRV *.OVL │
│ │ 09/19/95 16:13 All Mac Files Will Be Checked                 │ │
│ │ 09/19/95 16:13 Infected Files Will be Recorded               │ │
│ │ 09/19/95 16:13 Delay If CPU Utilization Up to: 25  Scan Type: Secure │
│ │ 09/19/95 16:13 Traverse Directory: Yes                       │ │
│ │ 09/19/95 16:15 [DOS][SYS:\ACCTNG\ PAYMNT.EXE ] Infected with Virus [Friday 13th │
│ │              12,779 KBytes  in 154 Files in 86 Directories Have Been Scanned │
│ │              1 Virus Detected In 1 File                      │ │
│ │              No Action Taken                                 │ │
│ │              Total Elapsed Time : 00:02:14                   │▼│
│ └─────────────────────────────────────────────────────────────┘ │
│ ◄───────────────────────────────────────────────────────────► │
│           ┌───────┐      ┌───────┐      ┌───────┐               │
│           │ Print │      │ Close │      │ Help  │               │
│           └───────┘      └───────┘      └───────┘               │
└─────────────────────────────────────────────────────────────────┘
```

Scan Record settings

InocuLAN will keep from 10-2,000 records. When the file is full, the records will be purged in date sequence (oldest first). You can also set how long you wish to keep a record.

To set the Scan Record options:

1. **Click the Configuration button in the Domain Manager window.**

2. **Click the Scan Record/Event Log tab.**

```
┌─────────────────────────────────────────────────────────────────┐
│ ─ │                    Configuration                             │
├─────────────────────────────────────────────────────────────────┤
│ ┌──────────────┬───────────┬────────┬────────────────────────┐  │
│ │Realtime Monitor│ Enforcement │ Server │ Scan Record/Event Log │  │
│ │┌Scan Record─────────────────────────────────────────────────┐ │
│ ││ ┌General──────────────────┐  ┌Message Filters───────────┐  │ │
│ ││ │                         │  │ ☒ Log Critical Messages  │  │ │
│ ││ │ Maximum Messages: 100 ▲ lines│ ☒ Log Warning Messages │  │ │
│ ││ │                       ▼ │  │                          │  │ │
│ ││ │ Purge Records Time: 30 ▲ days│ ☒ Log Informational Messages │ │
│ ││ │                       ▼ │  │                          │  │ │
│ ││ └─────────────────────────┘  └──────────────────────────┘  │ │
│ │└────────────────────────────────────────────────────────────┘ │
│ │┌Event Log───────────────────────────────────────────────────┐ │
│ ││ ┌General──────────────────┐  ┌Message Filters───────────┐  │ │
│ ││ │                         │  │ ☒ Log Critical Messages  │  │ │
│ ││ │ Maximum Messages: 200 ▲ lines│ ☒ Log Warning Messages │  │ │
│ ││ │                       ▼ │  │                          │  │ │
│ ││ │ Purge Records Time: 30 ▲ days│ ☒ Log Informational Messages │ │
│ ││ │                       ▼ │  │                          │  │ │
│ ││ └─────────────────────────┘  └──────────────────────────┘  │ │
│ │└────────────────────────────────────────────────────────────┘ │
│ │   ┌──────┐   ┌────────┐   ┌───────┐   ┌──────┐                │
│ │   │  OK  │   │ Cancel │   │ Apply │   │ Help │                │
│ │   └──────┘   └────────┘   └───────┘   └──────┘                │
└─────────────────────────────────────────────────────────────────┘
```

3. Select the Scan Record options.

Maximum Messages — The maximum number of messages that should remain in the Scan Record. Values range from 10 to 2,000 lines.

Purge Records Time — Indicates how long, in days, you want to keep an event in the log. Values range from 1 to 365 days.

Message Filters — You can select the type(s) of message(s) that should be stored in the Scan Record.

Message Type	Description
Critical Message	This is the highest level message. It requires your immediate attention once logged. This message could mean, for example, that a virus was detected, or there is a critical problem on the network. This is the default and cannot be unchecked.
Warning Message	The second priority message tells you if a scan was cancelled and no virus was found at that point.
Informational Message	This will tell inform you of events that do not require a response, such as a scan has started or stopped, or a completed scan found no viruses.

4. Click OK when done.

Using the Local Scanner

The Local Scanner scans files on a local workstation or a server. The server to be scanned does not have to be an InocuLAN server, but you must be connected to the server. The actual scanning is done by the InocuLAN for Windows Manager on the local workstation. This component is not automatically installed, see Appendix C for installation instructions

> NOTE: You cannot use the Local Scanner on a server that has real-time scanning enabled with the outgoing files option selected. Viruses will be reported by the Real-time Monitor. Instead, you can use the Domain Manager for these servers.

Instructions for a basic scan

Follow the instructions below to perform a basic scan (without any options or filters) using the Local Scanner. Information about installing the Local Scanner on workstations is in Appendix C. Information about using options and filters begins in the next section.

1. Click the Local Scanner button.

    InocuLAN reads all of the directories on the drive where InocuLAN's home directory is located before the Local Scanner screen appears:

Half shaded
target boxes
indicates a partial
volume scan
selection.

If a volume is
displayed with a
green border and
the letter R in
blue, the volume
is protected by the
Server Real-time
Monitor program.

Click the light blue
selection boxes
to green to
choose a drive or
mapped volume
to scan for
viruses.

Cheyenne AntiVirus - [Local Scanner]

File   Scan   View   Window   Help

Directories:

- C:\
- D:\
- E:\
- F:\ (NY-ENG\SYS)
- H:\ (NY-PICARD\WATSON)
  - INOCULAN.QA
    - 20.42
    - 20.47
    - 20.48
    - 20.49
    - 20.50
    - 20.51
    - 20.53
    - 20.54
    - 21.10
    - 21.11

Files:

File name	File Size	Modified
COMMAND.COM	92870	07/11/95 09:50 AM
CONFIG.SYS	69	05/19/97 04:06 PM
CSTARTUP.EXE	30720	05/01/96 02:00 AM
IO.SYS	223148	07/11/95 09:50 AM
IOU.SYS	4	03/18/97 06:23 PM
MSDOS.SYS	1646	05/20/97 02:12 PM
WD1	0	03/29/96 06:02 PM
WO1	214	03/29/96 06:09 PM
WZT1	11	06/24/96 11:09 AM

5/20/97   3:33:32 PM

Displays volume
information.

A file with a magnifying glass indicates
a targeted file for a scan job.

2.   Select what to scan.

The entire drive is automatically selected for you.
You can scan this drive or you can select another.

If you want to scan the entire drive, but you want to
exclude a specific directory, double-click on that
directory.

If you only want to scan specific files or directories,
double-click the drive letter (to de-select everything)
and then double-click on each file or directory you
want to scan. If you are selecting specific files, the
files must ALL be in the same directory.

Start

3.   Click the Start button.

The scan begins immediately.

Stop

After the scan begins, the Start button turns gray, and the Stop button turns red. Click the Stop button at any point to stop the scanning process.

Options for Workstation Scans

To apply an option:

1. Click the Configuration button on the Local Scanner screen.

   The Local Scanner Options screen appears:

   Local Scanner Options

   | Options | File Types |

   Objects to Scan:
   ☒ Boot Sector   ☒ Files

   Options:
   ☒ Automatically display results
   ☒ Prompt On Action
   ☒ Sound Beep on Detection
   ☒ Generate Scan Records

   Check this box to enable or disable the Scan Records option.

   Action Upon Virus Detection:
   Report Only - No Action

   Rename Extension: AVB
   Move Folder:
   C:\INOCNEW\VIRUS

   ☐ Customized message
   Virus detected, please call MIS

   Scan Type:
   ⦿ Fast Scan   ○ Secure Scan   ○ Reviewer Scan

   OK   Cancel   Apply   Help

   Check this box the enable Customized message option to be displayed upon virus detection. Type in the field provided to display your personal message.

2. Select the options you want to include with the scanning job.

   Objects to Scan   You can select to scan the boot sector (which contains code that is executed when the system is booted) and/or files.

NOTE: Some options like the Splash Screen disable box, the Mapped Drive information box, or the Change Configuration enable box on the InocuLAN AntiVirus Scanner program are not enabled until the InocuLAN servers and workstations are updated with the AVUPDATE program. For further information on these options, please refer to your AVUPDATE manual.

File Selection

Select the File Types tab on the Local Scanner Option menu to choose from 5 different file types to be filtered or scanned. This menu will appear:

Local Scanner Options

Options | **File Types**

Dos File Selection

Executable Files Only ▼

All Files
Specified Extensions Only
Extensions Excluded
Use Filter
Executable Files Only

DRV
EXE
OVL

Delete

File filter
.

Compressed Files

☒ Scan Compressed Files

File Extensions:

ARJ
ZIP

Add

Delete

OK | Cancel | Apply | Help
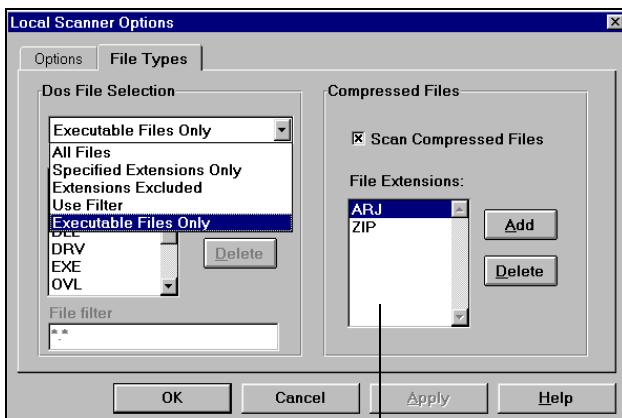
You can also add various file compression types to be included in the scan job.

You can select *All Files*, *Specific Extension Only, Extension*s *Excluded, Use Filter*, or a selection of *Executable Files Only*. If you select *Specified Extensions Only* option, you can further define which files to scan by their extensions. If you select the *Use Filter* option, you can insert asterisks (*) in the **File Filter** field to represent a wildcard filter.

Action Upon Virus Detection

Select one of the options described below. (Regardless of which option you choose, a message will be broadcast when a virus is detected.)

Action	Description
Report Only - No Action	Displays an on-screen report that lists the infected files and the virus that was detected. This information also appears in the Scanning Report.
Delete File	Deletes an infected file from a workstation.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to 'Rename File' below). Even if InocuLAN cures the file, we recommend you purge the infected file and then restore the original file.
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory.
Purge File	Deletes an infected file so that it cannot be recovered.
Rename File	Renames infected files by giving them an .AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners (except the Real-time Monitor). If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Copy and Cure File	Will make a copy of the infected file to the INOCULAN\VIRUS directory and continues to cure the file.

Action	Description
Rename and Move File	Renames infected files by giving them a different extension and then moves them to the INOCULAN\VIRUS directory.

NOTE: If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

Automatically Display Results

Select this option if you want to have the results of the scan displayed on the screen.

Prompt on Action

Select this option if you want to be notified before InocuLAN takes any action with infected files.

Sound Beep on Detection

Select this option if you want your workstation to beep when a virus is detected.

Scan Type

Select one of the following scan types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan*. Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.

Scan Type	Description
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected.

Scan Compressed Files

Select this option to scan compressed files. By default, InocuLAN will scan compressed files of the .ZIP and .ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, click the Add button.

3. Click OK when done.

Checking the Results of Your Scan

If you have the option *Automatically Display Results* selected, the results of your scan will appear on the screen when the scan is completed.

This screen appears when the scan is finished.

Virus Scan Results

Scan Summary:

Dirs:	78	Start:	00:10:16	OK
Files:	398	Stop:	00:11:19	Help
Viruses:	1			
Boot Scan:	No	Elapsed:	00:01:03	

Boot Sector:

Infections:	0
Cured:	0
Boot Sector Scanned.	

Files:

Infected:	1	Moved:	0
Cured:	1	Renamed:	0
Deleted:	0	Moved/Renamed:	0
Purged:	0		

Viruses Detected:

C:\REPORTS\INTERNET.EXE	Cascade virus
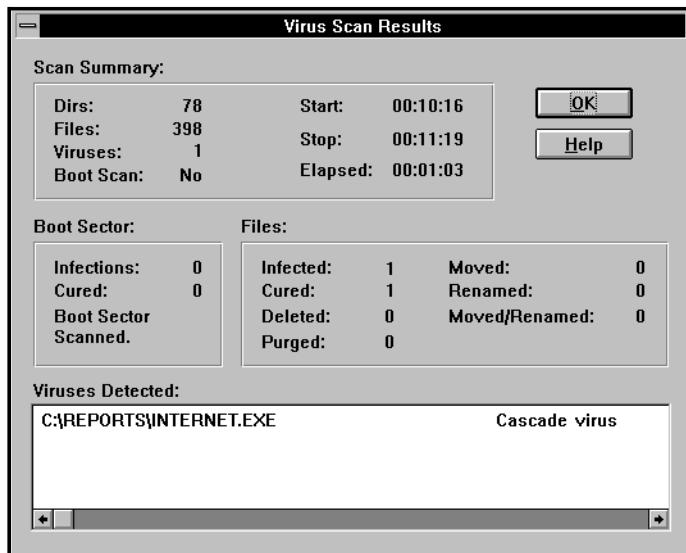
If you do not have this option selected, or if you want to view the results at a later time, follow the instructions on the next page.

1. Click the Reports button.

This screen displays the results of all Local Scanner jobs.

```
┌─────────────────────────────────────────────────────────────────────────┐
│ ─                     Local Scanner - Scan Log                           │
├─────────────────────────────────────────────────────────────────────────┤
│ Completed Time    │ Source Directory │ Virus │ Action       │ Status     │
│ ⓘ 11/19/95 4:04 PM │ C:\              │   0   │ Report Only  │ Completed  │
│ ⚠ 11/18/95 5:40 PM │ C:\              │   0   │ Report Only  │ Canceled   │
│ ☣ 11/17/95 4:41 PM │ C:\              │  21   │ Cure File    │ Completed  │
│ ☣ 11/17/95 4:30 PM │ C:\              │  22   │ Report Only  │ Completed  │
│                                                                          │
│                                                                          │
│ ◄                                                                      ► │
│   [Search]   [View]   [Print]   [Delete]   [Close]   [Help]             │
└─────────────────────────────────────────────────────────────────────────┘
```

Click to search the list for a specific job.

Click to view more detailed information about a job.

Click to print this list.

Click to delete the highlighted record.

2. Highlight the job you want to find out more information about.

3. Click View.

This screen displays detailed information about the scanning job.

```
┌─────────────────────────────────────────────────────────────────────────┐
│ ─          Record file: C:\INOCULAN\DB\IN000005.REC                     │
├─────────────────────────────────────────────────────────────────────────┤
│ *** InocuLAN Summary Listing (SCAN VIRUS) *** 11-17-1995 4:38 pm         │
│                                                                          │
│ No Boot Viruses Were Detected On Drive [C]                               │
│ Target Directory: [C:]                                                   │
│ [DOS][C:\COMMAND.CO2] was infected by virus [Junkie]                     │
│ Virus [Junkie] has been removed from [C:\COMMAND.CO2]                    │
│ [DOS][C:\BNETX.COM] was infected by virus [Junkie]                       │
│ Virus [Junkie] has been removed from [C:\BNETX.COM]                      │
│ [DOS][C:\COMMAND.COM] was infected by virus [Junkie]                     │
│ Virus [Junkie] has been removed from [C:\COMMAND.COM]                    │
│ [DOS][C:\DOS\DOSKEY.COM] was infected by virus [Junkie]                  │
│ Virus [Junkie] has been removed from [C:\DOS\DOSKEY.COM]                 │
│ [DOS][C:\DOS\COMMAND.COM] was infected by virus [Junkie]                 │
│ Virus [Junkie] has been removed from [C:\DOS\COMMAND.COM]                │
│ ◄                                                                      ► │
│              [Print]       [Close]       [Help]                          │
└─────────────────────────────────────────────────────────────────────────┘
```

3

GUARDING YOUR NETWORK WITH INOCULAN

An integral part of the process of keeping your network virus-free is preventing viruses from gaining access to your network.

In this chapter, you will learn:

Keeping Your Network Virus-free

While you can use InocuLAN *just* to detect and cure problems caused by viruses, the best way to keep your network virus-free is to prevent viruses from gaining access to your network in the first place.

InocuLAN features

InocuLAN offers many features that, when used together, provide a solid barrier against viruses. These features are discussed briefly below. Detailed information about each feature can be found in this chapter.

➤ **DOMAINS** allow you to group your InocuLAN domain servers so that they can share configuration information and resources. This helps you maintain your virus-free multi-server network with minimal effort.

➤ **REAL-TIME MONITOR** continually scans files on a domain server. Files can be scanned on an incoming or outgoing basis, or both.

➤ **WIMMUNE** scans files on a workstation for viruses each time a file is executed, accessed, or opened. It can also be set to monitor the workstation for virus-like behavior, such as unauthorized formatting of the hard disk. WIMMUNE can be used on all workstations, even workstations that do not have InocuLAN installed.
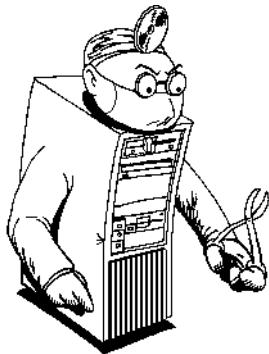
➣ **EXAMINE** is a program that checks a workstation for boot viruses. The workstation's Critical Disk Area is examined for changes, including infection and corruption.

➣ **ENFORCEMENT** prevents viruses from being copied to an InocuLAN/ NLM file server by forcing users to have WIMMUNE loaded before they can log into the server.

➣ **CRITICAL DISK AREA PROTECTION** safeguards a workstation's hard disk. The Critical Disk Area includes the boot sector, partition table, CMOS RAM information, and system files.

➣ **AUTOMATIC CHEYENNE BBS DOWNLOAD AND AUTOMATIC SERVER UPDATES** keep all of your InocuLAN servers synchronized with the most current virus signature files.

InocuLAN's scanners

In addition, InocuLAN has two scanning options that you can use to scan your network. They are discussed briefly below. Detailed information about these scanners can be found in Chapter 2, "Scanning your Network with InocuLAN."

➣ **Domain Manager** lets you administer scanning jobs on all of your domain servers. You can run the scan immediately or schedule it to start at a later time. Scanning can be repeated at regular intervals. This function is only available for supervisors or supervisor equivalents.

➤ **Local Scanner** scans files on a local
workstation or on a mapped drive. The
server does not have to be an InocuLAN
domain server.

General suggestions

In addition to all of InocuLAN's features, the following
general suggestions are offered to help keep your
network virus-free:

➤ Set all of your executable files as Read
Only files. Since a virus has the access
rights of the user, making these files
Read Only will reduce the chance of
executable files becoming infected with
viruses by non-supervisor users.

You can also use the more restrictive
Execute Only option for executable files.
*Make sure you are aware of the
restrictions that may apply to these files.*
For example, when you set a file to
Execute Only, you may not be able to
remove this setting, or back up the file.
Refer to your *Novell Utilities Reference
Manual* for more information about
setting rights before you proceed.

➤ Be careful with supervisor privileges.
Logging in as a supervisor or having
supervisor-equivalent privileges gives
you access to the file server's directory
structure. This means you can infect the
entire directory structure if your
workstation is infected with a virus.
Therefore, you should not log in as a
supervisor unless you actually need
supervisory privileges to perform a task.

➤ Do not grant users read, open, or search rights to other users' directories. Viruses can be spread if a user executes an infected program or copies an infected file from another directory.

➤ Cold-boot your workstation from a write-protected, virus-free boot diskette before running InocuLAN.

➤ Use InocuLAN to scan floppy diskettes for viruses before copying any files from them.

➤ Back up your network after you successfully scan the network for viruses. This way, if InocuLAN detects a file with a virus that cannot be cured, you can restore a backed up version of that file.

Domain Management

What is a domain?
A domain is a group of one or more InocuLAN servers (servers with InocuLAN installed) that can share configuration information and resources. Each domain contains one *master server*. All other servers in a domain are considered *member servers*.

What are the benefits of a domain?
A domain can be managed as a single entity. This has several benefits:

> You only have to enter configuration information once as all domain information is stored in the master server, and automatically configures all of your member servers at the same time. (If necessary, each member server can have its own configuration.)

> Using InocuLAN's Domain Scanner, you can scan all of your domain members by setting up one scan.

> All of the scanning reports on member servers are collected by the master server. Therefore, from your master server, you can see all of the activities of your member servers.

What type of information is shared by domain members?
The following is shared by all members of a domain:

> Real-time Monitor configuration

> Domain Manager configuration

> Activation/Deactivation of InocuLAN NLM

> Enforcement list

Creating an InocuLAN Domain

In order to enjoy the benefits of a domain, you must create a domain.

NOTE: Before you can create a domain, you must install InocuLAN on each server that will be in your domain.

Do the following to create a domain:

1. Click the Domain button

    The Domain Manager screen appears:

This is an expanded multi-server domain.

This is an available server.
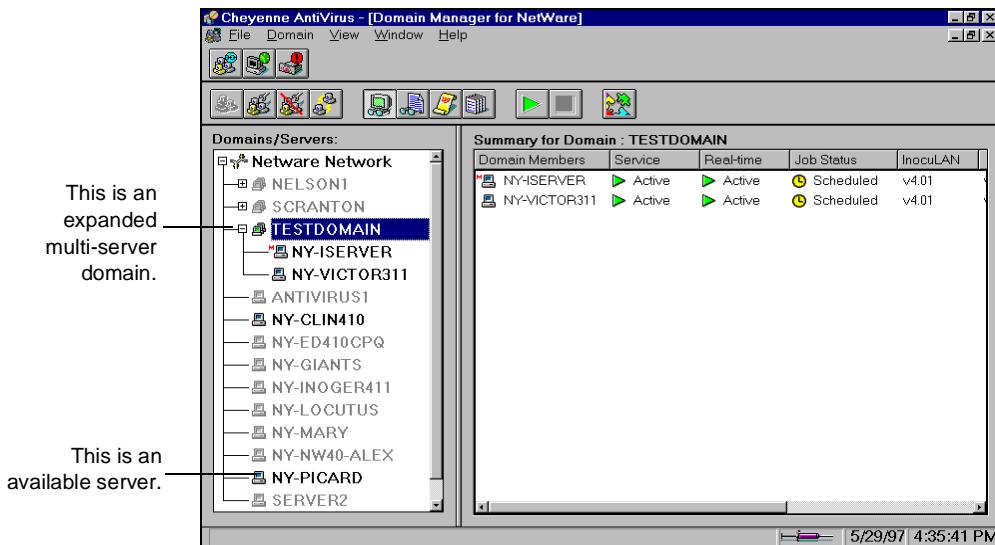
2. Highlight the server that will become the master.

3. Click the Create Domain button.

    The Create Domain screen appears.

4. Enter information about the new domain.

Enter a name for the domain.

The server you selected
becomes the master server by
default. If necessary, you can
select a different master server.

Create Domain

Name:

Master:
NY-ISERVER

Members:

Available Servers:
NY-LOCUTUS

<< Add

Remove >>

OK

Cancel

Help
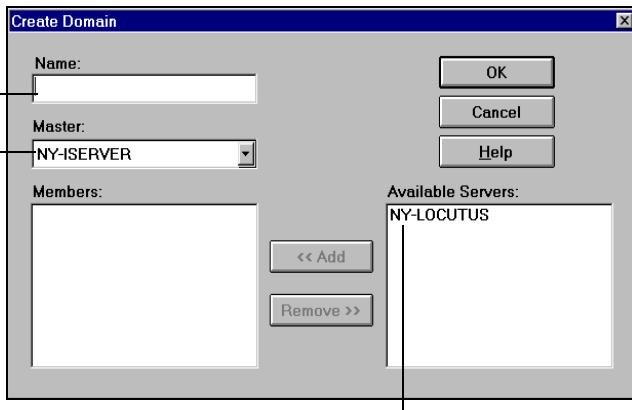
To add domain members, highlight an
available server and click the Add button.

5.   Click OK when done.

Checking the status
of domain members

To see the status of a server in an existing multi-server
domain:

1.   Highlight a domain.

2.   Highlight a member server listed in the Domains/Servers
window.
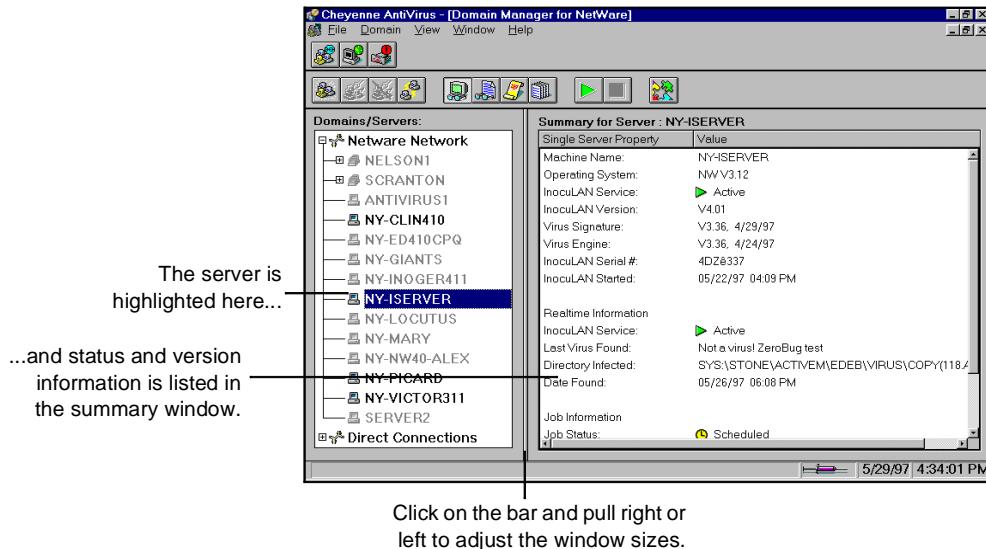
The server is highlighted here...

...and status and version information is listed in the summary window.

Click on the bar and pull right or left to adjust the window sizes.

Real-time Monitoring on the Server

The Real-time Monitor scans files on a domain server in real-time. Files can be scanned on an incoming or outgoing basis, or both.

Your Real-time Monitor configuration will be shared by all members of the domain.

Follow the instructions below for configuring the Real-time Monitor:

1. Click the Domain button.

2. Highlight a domain.

3. Click the Configuration button.

   The Real-time Monitor page of the Configuration window appears:
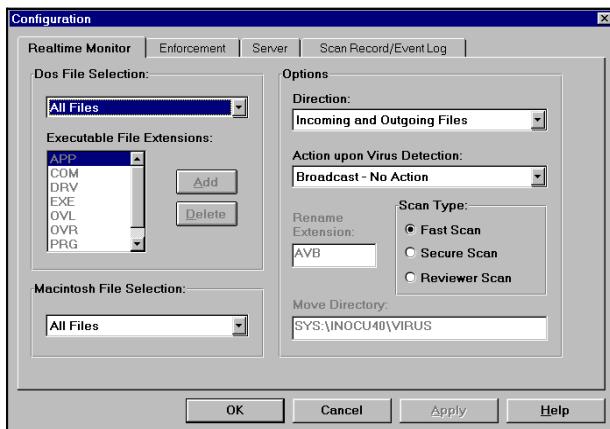
4. Select the options you want.

File Selection	You can select *All Files* or a selection of executable files. If you select *Executable Files*, you can further define which files to scan by their extensions.

Click the Add button to enter an executable file type.

To delete a file type from the list, highlight it and click Delete.

Macintosh File Selection	You can select all files, application type files, or files with a resource fork (the portion of a Macintosh file that contains the program code, font information, and other data not normally generated by a user). You can also choose not to scan Macintosh files.

Indicate when files should be scanned.

Setting	Description
Incoming files	Files being copied to the server and files being opened for writing on the server are *incoming*. Incoming files are scanned after the file is closed.
Outgoing files	Files being copied from the server and files that are being executed from the server are *outgoing*. Outgoing files are scanned when the file is opened. If the file is found to be infected, you will be denied access to it.
Incoming and Outgoing Files	Scans both incoming files and outgoing files.
Disable	This setting will disable the Real-time Monitor.

Action upon Virus Detection	Select one of the following options. Regardless of which option you choose, a message will be broadcast when a virus is detected.

NOTE: InocuLAN's Alert system can be configured to send a message to people in your organization when a virus is encountered. Messages can be sent via pager, e-Mail, FAX, NetWare broadcast, SNMP, or trouble-tickets sent to a printer. This assures that any viral infection on your network is immediately communicated to the people responsible for taking corrective actions. To configure the Alert service, refer to Chapter 4, "Alerting Users If a Virus is Detected."

Action	Description
Report Only - No Action	Sends messages to Alert via Broadcast, Fax, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Report Log.
Delete File	Deletes an infected file from the machine.
Rename File	Renames infected files by giving them an .AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners. If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to 'Rename File' below). Even if InocuLAN cures the file, we recommend you purge the infected file and then restore the original file.

Action	Description
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory.
Purge File	Deletes an infected file so that it cannot be recovered (for example, using Novell's Salvage utility).
Rename and Move File	Renames infected files by giving them a different extension and then moves them to the INOCULAN\VIRUS directory.

NOTE: An infected Macintosh file cannot be renamed or moved.

Every Macintosh file has a file type. If a virus is found, the file type is changed to prevent the file from being used and prevent the virus from spreading. The file types are:

Macintosh File Type	New File Type
Application - APPL	INOA
Data - DATA	INOD
Resources - RSRC	INOR
Stack - STAK	INOS
Text - TEXT	INOT

Scan Type   Choose one of the following scanning options:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

5.   Click OK when done.

The real-time scanning configuration will take effect immediately.

Recovering from a virus

If the Real-time monitor finds a virus, you must begin proper virus recovery procedures. See Chapter 11, "Virus Recovery Procedures," for details.

Real-time Monitoring of the Workstation with WIMMUNE

The WIMMUNE program, a real-time monitor, is a VxD (Virtual Device Driver) program that scans files on your workstation for viruses each time a file is executed, accessed, or opened. It also monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk.

If WIMMUNE finds an infected file, a window will pop up on your screen to inform you. The message will display the name of the infected file and the name of the virus.

Automatic loading of WIMMUNE

When InocuLAN was installed on your workstation, WIMMUNE was configured to start automatically when you start Windows. This helps ensure protection against viruses.

IMMUNE's Active Monitor window

While you are in Windows, WIMMUNE's Active Monitor keeps track of viruses that are discovered on your workstation. You can view this monitor at any time by selecting *InocuLAN-Active Monitor* from your Windows Task List or by double-clicking the icon when the Monitor is minimized.

```
┌─────────────────────────────────────────────────────────┐
│ ─      Cheyenne InocuLAN - Active Monitor          ▼│▲ │
│ Help                                                      │
│ ┌───────────────────────────────────────────────────────┐│
│ │ Total number of viruses found:                        ││
│ └───────────────────────────────────────────────────────┘│
│ ┌───────────────────────────────────────────────────────┐│
│ │ Last virus found:                                     ││
│ └───────────────────────────────────────────────────────┘│
│ ┌───────────────────────────────────────────────────────┐│
│ │              On file:                                 ││
│ └───────────────────────────────────────────────────────┘│
│ ┌───────────────────────────────────────────────────────┐│
│ │ Last virus type:                                      ││
│ └───────────────────────────────────────────────────────┘│
│ ┌───────────────────────────────────────────────────────┐│
│ │ Type of InocuLAN IMMUNE loaded: Large, Extended       ││
│ └───────────────────────────────────────────────────────┘│
│              ┌─────────────────────────┐                 │
│              │  Disable Active Monitor │                 │
│              └─────────────────────────┘                 │
└─────────────────────────────────────────────────────────┘
```

Enable or disable the
Active Monitor by clicking
the toggle button.
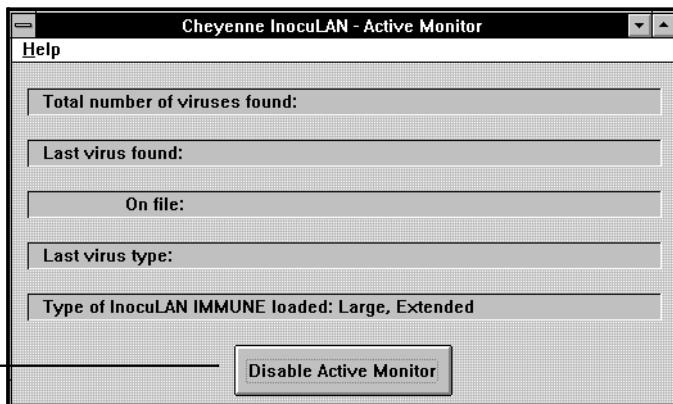
Disabling the Active Monitor	You can disable the Active Monitor by clicking on the toggle switch in the center of the window. Clicking it again will re-enable the Active Monitor.
WIMMUNE and Enforcement	The WIMMUNE program plays an important role in keeping your network free of viruses. When used with the Enforcement option, all Windows users logging in to a domain must have WIMMUNE running, or they will be disconnected from the network. This prevents unprotected users from infecting the network. See 'Using Enforcement' on page on page 3-17 for details.
Virus recovery procedures	If WIMMUNE locates a virus, you must begin proper virus recovery procedures. See Chapter 11, "Virus Recovery Procedures," for details.

Using Enforcement

Enforcement adds more security to your network by preventing viruses from being copied to an InocuLAN server. It does this by forcing users to have WIMMUNE loaded (or IMMUNE, for DOS users) and active before they can log in to the server.

If a user tries to log in to the server without having WIMMUNE loaded, messages will be sent to the user informing him or her to load WIMMUNE or be disconnected. The amount of time during which the user will receive these messages is called the grace period. The default grace period is 60 seconds, which can be modified using the Domain Manager.

Enforcement is not
active initially

When InocuLAN is first installed, the Enforcement option is not active. All users are allowed to log in to the domain server. You should activate Enforcement once users have access to WIMMUNE.

Activating
Enforcement

Enforcement can only be activated if the InocuLAN Server is loaded. Do the following to activate Enforcement:

1. Click the Domain button.

2. Highlight a domain.

3. Click the Configuration button.

4. Select the Server tab.

5. Click the Enforcement Active check box to activate Enforcement.

Configuration

| Realtime Monitor | Enforcement | **Server** | Scan Record/Event Log |

Server Parameter

☒ Server Active

☐ Auto Update Signature

☒ Send Alert to Local Server

☒ Enforcement Active

Update Domain Interval   `60`   minutes

Grace Period: `60`   seconds.

NCOPY Delay: `1000`   ms.

Job Queue

Completed Job Hold Time: `1`   days.

Scan Queue Poll Interval: `10`   seconds.

OK   Cancel   Apply   Help

Click here to activate Enforcement.

If you are experiencing problems when performing large scanning job, you can increase the NCOPY Delay time interval to give the virus scanner program more time to finish its functions.
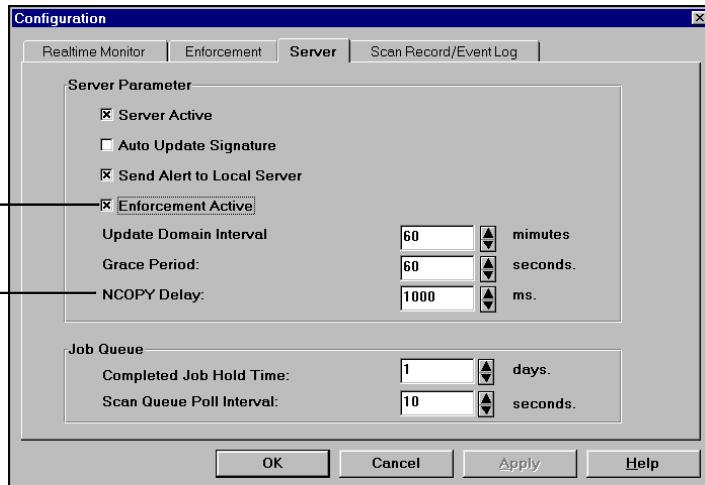
NOTE: Workstations without WIMMUNE loaded and active will be disconnected after Enforcement is activated and the grace period elapses.

6. Click OK to save your selections.

Excluding users and groups from Enforcement

In order to be flexible, InocuLAN allows certain users and groups to be exempt from Enforcement. This may be necessary for certain remote users or workstations that do not have enough memory for WIMMUNE.

As a default, the user "Supervisor" is excluded from Enforcement. If other people tend to use the Supervisor's ID, you may want to remove it from exclusion.

If you are using domains, your Enforcement list will be shared by all members of the domain.

To exclude users or groups from Enforcement:

1. Highlight a domain.

2. Click the Configuration button.

3. Select the Enforcement tab.

   The Enforcement screen appears:
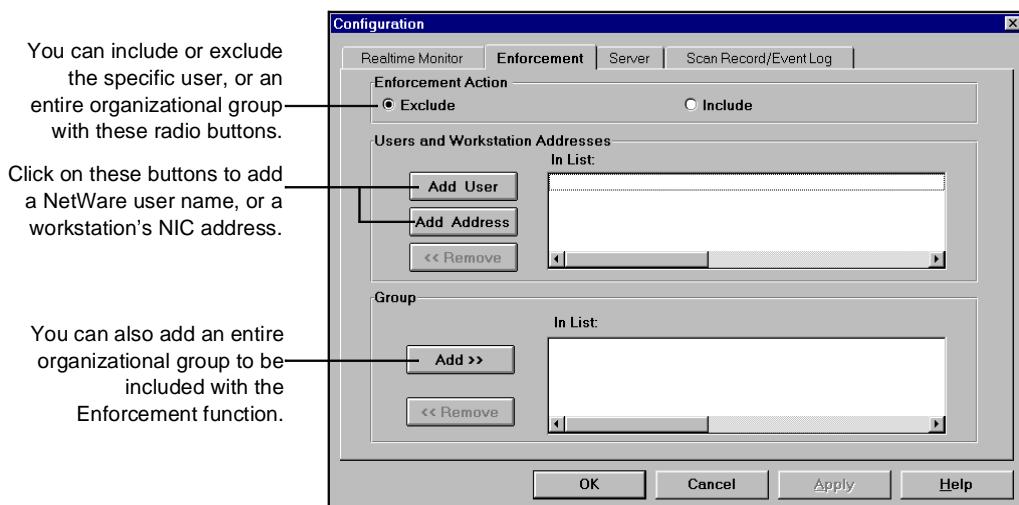
You can include or exclude the specific user, or an entire organizational group with these radio buttons.

Click on these buttons to add a NetWare user name, or a workstation's NIC address.

You can also add an entire organizational group to be included with the Enforcement function.

The Enforcement screen allows you to configure enforcement in two ways: by building a list of Users and Groups and then deciding if you want to *Exclude* or *Include* them.

To add an user's name just click on the **Add User** button and a field will pop up prompting you to enter the specific NDS name.

To add a workstation to the *In List*, you can click on the **Add Address** button to prompt for a NIC card address entry field.

You can even add an entire NetWare organizational group to the *In List* to be included with the

Enforcement functions by click on the **Add >>** button under *Group*.

Further information is provided in the field definitions that follow:

Enforcement Action

Exclude - This will exclude from Enforcement all users, groups and/or workstation addresses found in the *In List* window. In other words, the *In List* entries will *not* be forced off the network if they don't have WIMMUNE or IMMUNE running.

Include - This will *include* all users, groups and/or workstation addresses found in the *In List* window. In other words, the *In List* entries *will be forced off the network* if they don't have WIMMUNE or IMMUNE running.

User or Group

The *In List* windows determine which users, groups and/or workstation addresses will be subject to Enforcement, depending on the Enforcement Action selected.

The following chart explains the possible combinations:

Enforcement Action	In List/Not In List
Exclude	*In List* - These entries will *not* be subject to Enforcement. In other words, they will not be forced off the system if they don't have WIMMUNE or IMMUNE running. *Not in List* - These entries *will be* subject to Enforcement. In other words, they will be forced off the system if they don't have WIMMUNE or IMMUNE running.

Enforcement Action	In List/Not In List
Include	*In List* - These entries *will be* subject to Enforcement. In other words, they will be forced off the system if they don't have WIMMUNE or IMMUNE running. *Not in List* - These entries *will not be* subject to Enforcement. In other words, they will not be forced off the system if they don't have WIMMUNE or IMMUNE running

Add Address	This button will place a workstation address into the *In List* window. A workstation address is useful for Enforcement purposes, because it will let you subject a *particular machine* to Enforcement, no matter what user has logged on using that machine.

Choosing this button will open the Add Workstation Address window. Enter a workstation address and click OK.

```
┌─────────────────────────────────────────┐
│ ─│        Add Workstation Address         │
├─────────────────────────────────────────┤
│ Workstation Address:                      │
│ ┌─────────────────────────────────────┐ │
│ │                                     │ │
│ └─────────────────────────────────────┘ │
│   ┌────────┐  ┌────────┐  ┌────────┐    │
│   │   OK   │  │ Cancel │  │  Help  │    │
│   └────────┘  └────────┘  └────────┘    │
└─────────────────────────────────────────┘
```
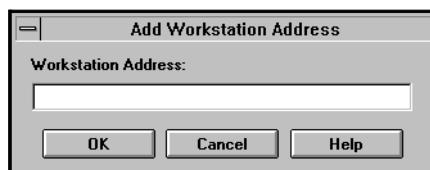
The workstation address is the 12-character NIC card node address, such as: `0000c08aed99`.

4. Make your Enforcement selections and click OK.

Deactivating Enforcement	**To deactivate Enforcement:**

1. Highlight a domain.

2. Click the Configuration button.

3. Select the Server tab.

4. Click the Enforcement Active check box to remove the check.

5. Click OK.

Changing the grace period for Enforcement	Enforcement uses a grace period, which is the amount of time the user has to load WIMMUNE before being disconnected from the server. The default grace period is 60 seconds.

You can change the grace period for Enforcement as follows:

1. Highlight a domain.

2. Click the Configuration button.

3. Select the Server tab.

4. Click and hold the up or down arrow next to the Grace Period field to increase or decrease the time allowed.

5. Click OK.

Viewing the Event Log

The Event Log contains information about the operations performed by InocuLAN. The log tells you when:

➤ InocuLAN is loaded on your server.

➤ A virus is discovered by WIMMUNE or the Real-time Monitor. (Viruses detected by the Workstation or Domain Scanners are reported in the Scanning Report.)

➤ The server's virus signature file is updated.

➤ Any configuration changes and operational results.

Although each InocuLAN domain server has its own Event Log, the master server's Event Log will report information about viruses discovered by WIMMUNE or the Real-time Monitor on member servers.

> NOTE: This is the same Event Log that you can view from the InocuLAN Server menu.

Displaying the Event Log

To display the Event Log:

1. Click the Domain button.

2. Highlight a domain.

3. Click the Log button.

The Event Log is displayed:

Click here to re-order the log
alphabetically by Event name.

*Information in the
log appears in
reverse
chronological*

Double-click on a log for more
information.

You can print the contents of the log by choosing
Print... from the Inoculan *File* menu.

Event Log Options

You can choose what kinds of messages the log will
record and the number of messages it will store.

To set Event Log options:

1. Click the Configuration button.

2. Click the Scan Record/Event Log tab.

Configuration

| Realtime Monitor | Enforcement | Server | Scan Record/Event Log |

Scan Record

General

Maximum Messages: `100`

Purge Records Time: `30`

Message Filters

☒ Log Critical Messages

☒ Log Warning Messages

☒ Log Informational Messages

Event Log

General

Maximum Messages: `200`

Purge Records Time: `30`

Message Filters

☒ Log Critical Messages

☒ Log Warning Messages

☒ Log Informational Messages

[OK] [Cancel] [Apply] [Help]

3. Select the Event Log options.

| Maximum Messages | The maximum number of messages that should remain in the Event Log. Values range from 10 to 1000 messages. |

| Purge Records Time | Indicates how long, in days, you want to keep an event in the log. Values range from 1 to 365 days. |

| Message Filters | You can select the type(s) of message(s) that should be stored in the Event Log. |

Message Type	Description
Critical Message	This is the highest level message. It requires your immediate attention once logged. This message could mean, for example, that a virus was detected, or there is a critical problem on the network. This is the default and cannot be unchecked.

Message Type	Description
Warning Message	The second priority message tells you if InocuLAN skips a file, and other non-critical information.
Informational Message	This will inform you of events that do not require a response, such as a scan has started or stopped, or a completed scan found no viruses.

4. Click OK when done.

Server Configuration

InocuLAN allows you to configure a number of server functions through the Domain Manager.

To configure the server:

1. Click the Domain button.

2. Highlight a domain.

3. Click the Configuration button.

4. Select the Server tab.

   The Server configuration window appears:
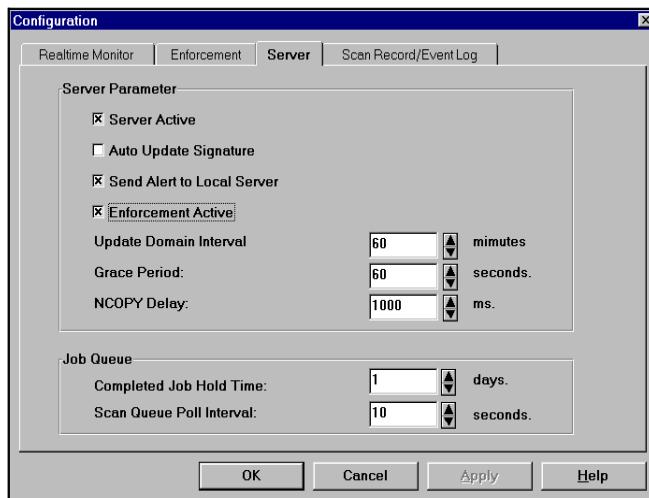
The following options are available:

Server Active   Select to activate InocuLAN on the server, or deselect to deactivate InocuLAN on the server.

Auto Update Signature	When selected, InocuLAN will automatically synchronize all of your InocuLAN domain servers with the most current version of InocuLAN's virus signature files.
Send Alert to Local Server	If the server is a member of a domain, entering YES will send alerts to the server, as well as to the master server.
Enforcement Active	When selected, Enforcement will be active for all workstations logging on to the domain. See 'Using Enforcement' on page on page 3-17 for details.
Update Domain Interval	Specifies the time that passes between each update of domain information. The values entered may be between 1 and 1,000 seconds.
Grace Period	Specifies the amount of time a user has to load WIMMUNE before being disconnected from the server. For more information, see 'Using Enforcement' on page on page 3-17.
Completed Job Hold Time	Specifies the time that a completed job will remain in the Job Queue record. The values entered may be between 1 and 30 days.
Scan Queue Poll Interval	Specifies the time that passes between each check of the scan queue. When the scan queue is checked, updated information is passed to the Domain Manager. The values entered may be between 1 and 60 seconds.
NCOPY Delay	When set to active, the NCOPY Delay function will hold the scan jobs for a specified amount of time in milliseconds. If you are experiencing problem with large scan job, you should set the NCOPY Delay to a higher setting.

> NOTE: When you perform a large scan job through the
> network, sometimes the Real-time Monitor will require a
> longer scan time to disinfect the files. If problems
> occurs, you can try setting NCOPY Delay to a longer
> time period.

5. Click OK when done.

Viewing Workstation Scanning Records

The Domain Manager allows you to view the workstation scanning records of all users logged in to the domain. In order to generate workstation records, one of two criteria must be present:

➣ The InocuLAN Manager is installed on the server, and not on the workstation.

➣ The AVUPDATE function is used with the U option. (See page on page 3-42 for details.)

To view workstation scanning records from the Domain Manager:

1. Click the Domain button.

2. Highlight a domain.

3. Click the Workstation Scan Record view button.

   The Workstation Scan Record window appears:

Click on a field heading to arrange the records based on the heading topic.

Double click on the individual workstation to view its scanning records.

The scan summary is listed by machine name and user login name. The number of Critical, Warning and Informational messages in each scan record is shown. A Critical message may mean a workstation has a virus.

4. Click on a workstation entry to access the workstation scanning record.

If any viruses were found on a workstation, it is clearly indicated in the scanning report.

	Completed Time	Source Directory	Virus	Action	Status
🔵	11/27/95 11:10 AM	C:\	0	Report Only	Completed
🔵	11/24/95 2:15 PM	C:\	0	Report Only	Completed
🔵	11/22/95 2:38 PM	C:\	0	Report Only	Completed
🔵	11/21/95 5:32 PM	C:\	0	Report Only	Completed
🔴	11/20/95 11:15 AM	C:\	4	Purge File	Completed
🔴	11/20/95 11:03 AM	C:\	4	Report Only	Completed
🔵	11/18/95 11:19 AM	C:\	0	Report Only	Completed
🟡	11/18/95 11:19 AM	C:\	0	Report Only	Canceled
🔵	11/18/95 9:52 AM	C:\	0	Report Only	Completed
🔵	11/18/95 9:52 AM	C:\	0	Report Only	Completed
🔵	11/18/95 9:52 AM	C:\	0	Report Only	Completed
🟡	11/18/95 9:51 AM	C:\	0	Report Only	Canceled

Workstation Scan Record for Workstation: 00000102-0000c0920880

[Search] [View] [Print] [Delete] [Close] [Help]

You can easily see the scans that reported a virus or a Critical message.

5. Click on a selected record to view scan details.

View Record #7

```
*** InocuLAN Summary Listing (SCAN VIRUS)  *** 11-20-1995 11:03 am

No Boot Viruses Were Detected On Drive [C]
Target Directory: [C:]
[DOS][C:\MANUALS\MERCURY\MISC\MERC.DOC] was infected by virus [WinWord.C
[DOS][C:\MANUALS\MERCURY\MISC\~WRL2149.TMP] was infected by virus [WinWd
[DOS][C:\MANUALS\MERCURY\MISC\APPB.DOC] was infected by virus [WinWord.C
[DOS][C:\MANUALS\MERCURY\MISC\~WRL3305.TMP] was infected by virus [WinWd

Total Files Scanned:        2,165
Total Bytes Scanned:        110,147,647
Total Viruses Found:        4
Total Infected Files Found: 4
Scan Type:                  Secure
Total Elapsed Time:         00:01:50
*** End Of Summary ***
```

[Print] [Close] [Help]

Protecting your Critical Disk Area

The Critical Disk Area of a workstation includes the Boot sector, Partition Table, CMOS RAM information, I/O System file, system files, and Shell file (the COMMAND.COM in DOS).

The Critical Disk Area of a floppy contains the Boot sector. If the floppy is a bootable diskette, the Critical Disk Area also includes the I/O system file, DOS system file, and Shell file.

During the installation of the InocuLAN Manager, you had the opportunity to back up the Critical Disk Area of your workstation to a rescue diskette. In addition, this area is backed up to the InocuLAN home directory (the directory in which InocuLAN was installed).

Through the InocuLAN Manager, you can make a new backup of your Critical Disk Area, examine the area for viruses and changes, and restore the area from a backup. (A command line utility is also available. See 'Using the EXAMINE utility' on page on page 3-38.)

It is very important to maintain a current set of Critical Disk Area files for all workstations.

Back Up your Critical
Disk Area

Use *Back Up* to create a rescue diskette for a workstation. The diskette you use as a rescue diskette should be a DOS system diskette. The CONFIG.SYS on this diskette must have FILES=40 or a higher number.

You should back up your Critical Disk Area anytime you change your CMOS information, change your hard disk, or upgrade your operating system.

To back up your Critical Disk Area:

1. Click the Critical Disk Area button.

   The Critical Disk screen appears:

   Workstation Critical Disk Area : [Local]

   Boot Drive Information:

Drive:	C:\
Name:	ANDREW
Size:	206208 KBytes
Free:	31462 KBytes

   ormation about
   e appears here
   initially.
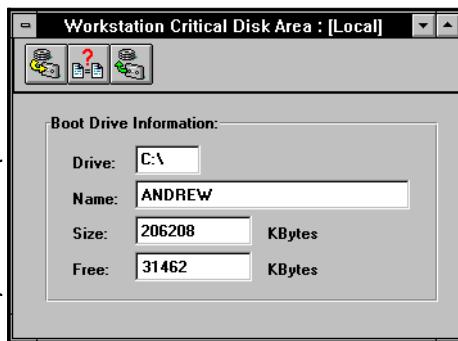
2. Click the Backup button.

3. Select a destination.

   You can select a drive, server or a domain.

   Critical Disk Area - Backup

   Backup Boot Drive To:

   - A:
   - C:
   - TEST2
   - TESTDOMAIN
   - NY-LOCUTUS

   Backup   Close   Help

   Select the drive, server or
   domain you wish to back up to.
   Note that double-clicking on
   your choice will start the backup
   process immediately.
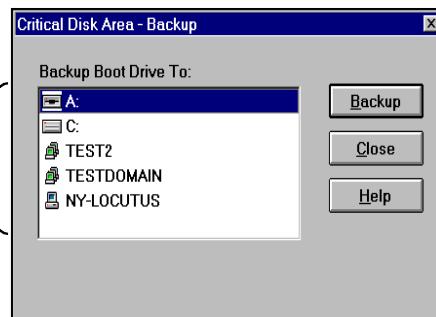
   If you back up workstations to a server or domain,
   the backup files will be placed in an InocuLAN
   subdirectory called CRITICAL.WS. The backup
   files for an individual workstation will be in a
   further subdirectory, named after the workstation
   address.

NOTE: If a workstation suffers damage to its Critical Disk Area and no diskette backup can be located, you can restore from the server if a server-based backup was performed. For this reason, it is a good idea to backup all workstations to both a diskette and a server.

4. Click Backup.

The Backup Activity screen will appear and the backup will begin.

This is the boot drive (the active partition in DOS).

This is the root of the drive selected or the InocuLAN home directory (if the drive selected is the drive where InocuLAN was installed).

Backup Activity

Boot Drive: C:

Destination: C:\INOCULAN\AUTOEXEC.SIG

Backing Up: AUTOEXEC.BAT

Backup Completed Successfully

OK

Help

The information that is backed up and the files that are created are listed below:

Information	File
CMOS settings	CMOS.SIG
Partition table	PARTSECT.SIG
Boot sector	BOOTSECT.SIG
DOS system file	DOS.SIG
DOS shell file	SHELL.SIG
BIOS system file	BIOS.SIG
AUTOEXEC.BAT file	AUTOEXEC.SIG
CONFIG.SYS file	CONFIG.SIG
Information about the above files and their location on the hard disk.	INFO.SIG

Use *Examine* to check your local bootable drives for viruses.

To examine your Critical Disk Area:

1. Click the Examine button on the Critical Disk screen.

Select the drive to be examined.

Select to compare your Critical Disk Area with a backed up version.

Indicate which drive or domain contains the backed up version.

```
┌──────────────────────────────────────────────┐
│ ─      Critical Disk Area - Examine           │
│ Examine Boot Drive:                           │
│ ┌──────────────────────┐   ┌──────────────┐  │
│ │ ▭ A:                 │   │  Examine     │  │
│ │ ▭ B:                 │   └──────────────┘  │
│ │ ▭ C:                 │   ┌──────────────┐  │
│ │                      │   │  Close       │  │
│ └──────────────────────┘   └──────────────┘  │
│                             ┌──────────────┐  │
│                             │  Help        │  │
│                             └──────────────┘  │
│ ☒ Also Compare Boot with Backup On:           │
│ ┌──────────────────────────────────────┐     │
│ │ ▭ A:                              ▲   │     │
│ │ ▭ B:                                  │     │
│ │ ▭ C:                                  │     │
│ │ ▭ D:                                  │     │
│ │ ▥ BLDG2                           ▼   │     │
│ └──────────────────────────────────────┘     │
└──────────────────────────────────────────────┘
```
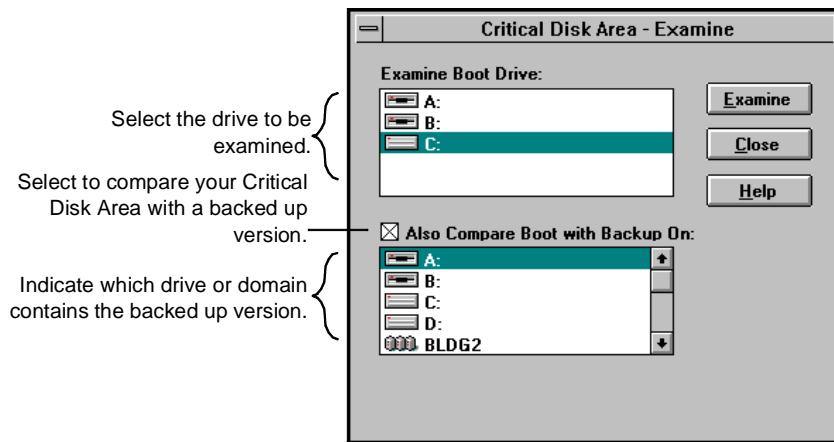
2. Select the drive to be examined.

You can also compare your boot drive with a backup made of the Critical Disk Area.

3. Click Examine.

The Examine Activity screen will appear and the examination will begin.

If a virus or change is detected in the Critical Disk Area you can use a rescue diskette to restore the area. (First check to see if there is a reason for a change in the area, such as a new version of you operating system.)

When the examination is complete, the "Examine Completed Successfully" message will appear on the Examine Activity screen.

Restore your Critical
Disk Area

Use *Restore* to recover from an infection or corruption of the Critical Disk Area.

NOTE: If you have a serious infection that will not allow you to boot your machine from the hard drive, see 'Critical Disk Area Lost' in Chapter 11, "Virus Recovery Procedures," for instructions.

To use the Restore function:

1. Click the Restore button on the Critical Disk screen.

2. Select the drive from which you want to restore.

The best place to restore from is a rescue diskette. If you do not have one, select the backup from the file server, if possible. Your last choice should be from your local hard drive.

3. Click Restore.

The Restore Activity screen will appear and the restoration will begin.

Using the EXAMINE Utility

EXAMINE is a command line utility that checks your workstation's hard disk for boot viruses. Your workstation's Critical Disk Area is examined for changes, including infection and corruption. The Critical Disk Area includes the boot sector, partition table, CMOS RAM information, and system files. EXAMINE also lets you back up and restore your Critical Disk Area. (These functions are also available through a Windows interface. See 'Protecting your Critical Disk Area' on page on page 3-33.)

You can execute EXAMINE by doing the following:

1. Type **EXAMINE** at the DOS prompt.

Automatic scanning with EXAMINE

EXAMINE is automatically run each time you boot your computer. This offers extra protection because your memory is scanned before other programs are loaded, thereby preventing a virus from spreading.

Using this command, EXAMINE will scan your Critical Disk Area each time you boot your workstation. You may add EXAMINE options to the above statement. For more information on these, see the Inoculan AntiVirus for NetWare Manual.

If EXAMINE locates a virus, you must begin proper virus recovery procedures. See Chapter 11, "Virus Recovery Procedures," for details.

Keeping your InocuLAN System Updated

Part of the process of safeguarding your network against viruses involves keeping your InocuLAN system up-to-date with the latest software available.

There will be times when Cheyenne Software makes an InocuLAN update available through Cheyenne's bulletin board, through CompuServe, or through a mailing. The update can contain new virus signature files (used by InocuLAN to detect viruses), or it can contain any number of InocuLAN files (including files for the domain server and files for the workstation).

Getting updates from the bulletin board

Cheyenne has one public InocuLAN directory on its bulletin board and on CompuServe. The name of the directory is UPDATE and it contains the latest virus signature files (VIRSIG.DAT or VIRUS.LST).

Get updates automatically with GETBBS.NLM

InocuLAN has an NLM that will automatically call Cheyenne's bulletin board and retrieve the latest update files for you. This NLM, GETBBS.NLM, can be installed on any server in your network. Whenever new virus signature files are retrieved by this NLM, InocuLAN will automatically update all member servers. For more information about configuring and using GETBBS.NLM, refer to Appendix B.

Updating your servers and workstations

In order to help you update all of your servers and workstations, InocuLAN offers the following:

- ➢ Automatic server updates of virus signature files.
- ➢ AVUPDATE - updates workstations.

➤ SUPDATE - updates servers with
various InocuLAN files.

Automatic server updates of virus signature files

If you have more than one domain server, InocuLAN
automatically synchronizes all servers with the most
current version of InocuLAN's virus signature files.

**Instructions for
updating just the virus
signature files**

If the update contains only the virus signature files
(VIRSIG.DAT and/or VIRUS.LST), do the following at one of
the domain servers:

1. Install the updates into InocuLAN Server's home directory
   on your InocuLAN domain server.

2. Select Update Virus Signature from InocuLAN's
   Configuration menu on the file server.

   This will not interfere with the operation of
   InocuLAN.

   After you do this, InocuLAN's automatic server
   update program will automatically update all of your
   domain servers for you, provided you enable the
   AUTO update feature.

Workstation updates using AVUPDATE

AVUPDATE.EXE can be added to the system login
script to automatically update InocuLAN files on
workstations as they log in to the domain server.
AVUPDATE.EXE uses AVUPDATE.DAT, which
contains a list of the updated files to be distributed.

During installation, this was done for you. The
following statement was added to your login script:

`#servername/vol:\home_directory\AVUPDATE.EXE`

For example, if InocuLAN is on SUNNY\SYS: in the INOCULAN directory, your statement would look like the following:

`#SUNNY/SYS:\INOCULAN\AVUPDATE.EXE`

When a user logs on to the server, the following prompt will be displayed:

Check Local InocuLAN Files Against Server Files <Y/ N>?

Responding YES will update the workstation files. You can prevent this prompt from appearing using the quiet mode option (see below).

Notes for NDS users

If you are using a login script with NetWare NDS, use the NETADMIN or NWADMIN utility to identify and select an object and edit the login script. If you are using options with AVUPDATE, they must be entered with a proceeding space, *not* with a slash or dash. See 'AVUPDATE Options' on the following page for option choices.

AVUPDATE options

There are several options available when using AVUPDATE. Options can be entered in the login script using a leading slash (/), dash (-), or space. For example, both of the following will work the same way:

#SUNNY/SYS:\INOCULAN\AVUPDATE.EXE /Q /U

#SUNNY/SYS:\INOCULAN\AVUPDATE.EXE Q U

Option	Description
Q	Quiet mode. AVUPDATE runs without issuing a prompt to the user. Workstation files will be automatically updated.
U	Update workstation scan records on the server. This will send current workstation scan record information to the server, where it can be viewed from the Domain Manager (accessible only via a supervisor ID). Using this option on all workstations will give the supervisor a centralized record of all workstation scanning activity.
W	Adds the group setup loading information to the Windows WIN.INI file. See 'Group Setup program' in Chapter 2 for details on implementing this option.
H -or- ?	Help option. This will display brief information about the Q and U options. The help option can be run from the command prompt when needed, but is not meant for use in the login script.

Server updates using SUPDATE

SUPDATE.EXE is run from a workstation. It allows you to distribute updated InocuLAN files installed on a single domain server to other domain servers on your network. SUPDATE.EXE uses SUPDATE.DAT, which contains a list of the updated files to be distributed. SUPDATE.DAT is located in the InocuLAN home directory on the server.

STOP

> NOTE: The InocuLAN NLM must be loaded before running SUPDATE.

Instructions for using SUPDATE

If the upgrade contains files other than the virus signature files, do the following:

1. Install the upgrades into InocuLAN Server's home directory on your InocuLAN domain server.

2. Run SUPDATE from a workstation by typing SUPDATE at the DOS prompt.

    SUPDATE.EXE is located in the InocuLAN home directory on your domain server. The following screen will appear after your network is scanned:

Version information for the virus signature file, engine file and InocuLAN version appears, along with current status (loaded or unloaded).

Every InocuLAN server on your network is listed.

```
Servers To Update                          Signature  Engine  NLM   Loaded
↑ NY-PET                                    U3.09     U3.09   U4.00  No
  NY-PETER                                  U3.09     U3.09   U4.00  No
  NY-PETER312                               U3.09     U3.09   U4.00  Yes
  NY-PRODM                                  U3.09     U3.09   U4.00  Yes
  NY-RU410                                  U3.07     U3.05   U4.00  Yes
  NY-SFT3                                   U3.10     U3.10   U4.00  No
  NY-SUNNY                                  U3.10     U3.10   U4.00  Yes
  NY-TSUPP04                                U3.07     U3.05   U4.00  No
  NY-TSUPP12                                U3.07     U3.05   U4.00  Yes
  NY-VICTOR311                              U3.10     U3.10   U4.00  No
  NY-WORF                                   U3.10     U3.10   U4.00  Yes
  NY-WRITER2                                U3.10     U3.10   U4.00  No
  NY41                                      U3.10     U3.10   U4.00  Yes
  PR-410B                                   U3.07     U3.05   U4.00  Yes
  PR-SOUTH                                  U3.07     U3.05   U4.00  No
↓ SERVER1                                   U3.10     U3.10   U4.00  No
```

3. Mark the servers you want to update.

   To mark all servers, press F6. To mark specific servers only, highlight a server and press F5.

   You can only highlight servers that have InocuLAN loaded. These servers will have YES in the Loaded column.

4. When you are finished, press F2.

   A prompt will ask you to verify the upgrade.

5. Enter the Supervisor ID and password for each server you have selected.

   A server cannot be updated without this information. This will prevent unauthorized tampering with your system.

```
┌─────────────────────────────────────────────────────┐
│        Enter Supervisor ID and Password for NY-SUNNY │
├─────────────────────────────────────────────────────┤
│ User Name: PETER                                     │
│  Password: ███████████████                           │
└─────────────────────────────────────────────────────┘
```

6. Indicate if you wish to reload the new files on the servers after they have been copied.

Depending on the files being copied in a given update, SUPDATE may reload the entire InocuLAN program or only selected files.

```
Do you want to reload InocuLAN Signature File on server NY-SUNNY?
No
Yes
```
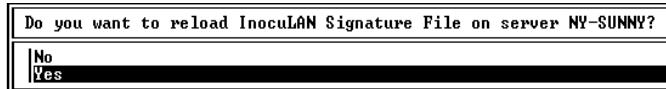
After choosing YES or NO for each server, the update process will begin. The progress of the update will be seen on screen:

```
                    Processing Server: NY-SUNNY
Copying INMEM.DAT ..
Copying SUPDATE.DAT .
Copying SUPDATE.HLP .
Updating.
```
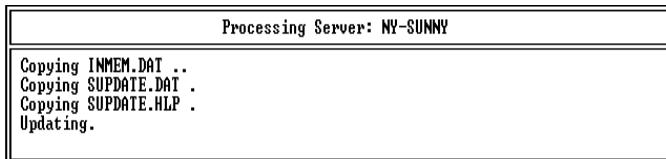
7. View and/or print the SUPDATE record.

    When completed, SUPDATE will issue a report detailing which servers were updated and what files were updated. To print this report, press F6 and enter a path and file name for the report. You can then print it using any appropriate word processor or text editor.

Multiple server capability allows for unattended updates

As described in the directions above, SUPDATE can be configured to update multiple servers in one process. All the necessary Supervisor IDs, passwords and reload instructions for all servers are entered at the start of the process. This allows the administrator to configure an update for as many servers as needed, start the process, and not have to watch for command prompts.

Three-step update provides extra safety

When updating files on a server, it is important that fail-safe measures are included in case of problems like a corrupted file or a bad sector on a disk.

The SUPDATE process involves three steps that ensure the utmost safety. The update process takes places as follows:

1. The new files are copied to the temporary storage subdirectory named DOWNLOAD.

    If there is a failure at this point, nothing is harmed because the working files have not yet been touched.

2. The corresponding old files are then copied to a subdirectory named BACKUP.

    If there is a failure at this point, nothing is harmed because the working files have not yet been touched.

3. The new files are then moved to the working directory, where they overwrite the corresponding old files.

    If there is a failure at this point, or after the files reload, you can easily recover by moving the old files from the BACKUP directory to the working directory, thereby overwriting any damaged files that may have been copied.

4

C h a p t e r

ALERTING USERS IF A VIRUS IS DETECTED

InocuLAN can alert you (or anybody you choose) whenever a virus is detected on your network.

In this chapter, you will learn:

Alert Basics

What is Alert?

Alert is a notification system that sends messages to people in your organization using different communication mechanisms. Alerts can be sent to the system administrator or anyone else, in or out of the office.

How does Alert work with InocuLAN?

InocuLAN uses Alert, a separate software program that is bundled with InocuLAN, to send alerts.

Alert does not generate its own messages. InocuLAN generates warning messages whenever a virus is detected. These warning messages are passed to Alert, which sends the notification.

Alerts can be sent via:

- ➤ Pager - Numeric and alphanumeric.
- ➤ FAX - FAXserve must be installed on the server through which you are sending the FAX. (FAXserve is a Cheyenne product that provides simple-to-use facsimile services for your network.)
- ➤ Electronic Mail - NetWare Message Handling System (MHS) must be installed on a server on your network.
- ➤ NetWare broadcasts - NetWare's broadcast system is used to send messages to specific users or groups.
- ➤ Trouble tickets - An alert can be printed through any print queue on your network. (Trouble tickets can only be sent to non-Postscript printers.)

> ➣ Simple Network Management Protocol (SNMP) managers - Such as NetWare ManageWise and HP OpenView.

Alert does not need to be loaded for InocuLAN to broadcast messages. The InocuLAN NLM will broadcast to all users defined in the NT_USER.DAT file, located in the InocuLAN home directory on the server. This file can be manually edited with an ASCII editor. The user name "Supervisor" is in the file by default. NetWare 4.x user names must be distinguished (complete) names, for example: ADMIN.ACCNTG.WORK.

What are the components of Alert?

Alert has three basic components:

> ➣ ALERT.NLM - This is the NetWare Loadable Module (NLM) responsible for the reception, processing, and distribution of alert messages.
> ➣ ALBUILD.NLM - This is the NLM that acts as the channel between Alert and other applications.
> ➣ *.ALT - This is the application profile file. This file is provided by an application (such as InocuLAN, which creates an INOCULAN.ALT file). This .ALT file must be present in the PUBLIC directory in order for Alert to handle messages generated by an application.

What do you have to do to generate alerts?

For InocuLAN to generate alerts, you must tell Alert what information must be communicated. For example, if you will be using the pager system, you will have to tell Alert what pager number to dial, and you will have

to supply information about your modem. All of this information must be configured in the Alert system on your master server. This configuration information is shared by all of your member servers.

Loading Alert

In order to use Alert, you must load it on your file server.

NOTE: To avoid loading unnecessary NLMs, Alert will not automatically load NLMs for all of its functions. Consult the following list and load NLMs for whatever functions you will be using. These NLMs must be loaded before the Alert NLM is loaded.

To use paging, load AIOCOMX.NLM and AIO.NLM
To use faxing, load FAXLIB.NLM
To use SNMP, load SNMP.NLM

To load Alert:

1.   Type **Load Alert** at the file server console.

Alert's main menu will appear:
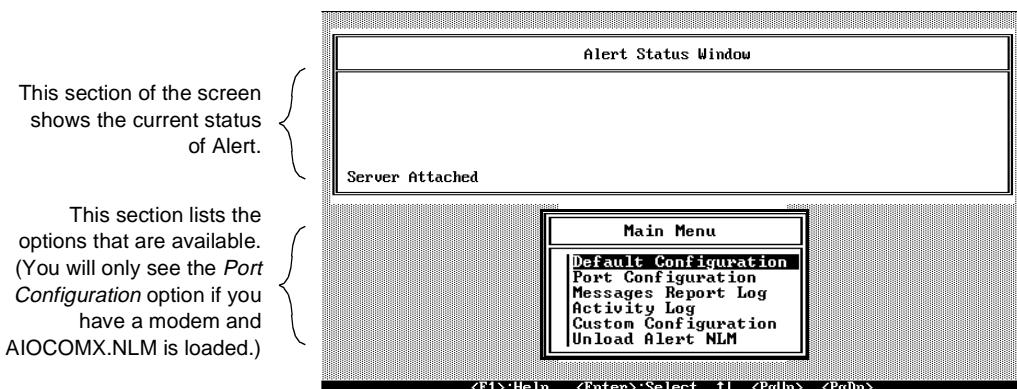
This section of the screen shows the current status of Alert.

This section lists the options that are available. (You will only see the *Port Configuration* option if you have a modem and AIOCOMX.NLM is loaded.)

```
                          Alert Status Window



Server Attached


                                 Main Menu
                          Default Configuration
                          Port Configuration
                          Messages Report Log
                          Activity Log
                          Custom Configuration
                          Unload Alert NLM
         <F1>:Help   <Enter>:Select  ↑↓  <PgUp>  <PgDn>
```

A brief description of each of Alert's menu options appears below. Detailed information can be found in the next few sections.

Default Configuration	This option allows you to set basic, default information about your Pager, MHS, FAXserve system, SNMP, modems, and printers.
Port Configuration	This option displays a menu that offers several modem options.
Messages Report Log	This option allows you to view a log containing messages that are processed by Alert.
Activity Log	This option allows you to view a log containing the status of Alert. While the current status is displayed on Alert's main menu, this log contains a historical listing of Alert's status.
Custom Configuration	This option allows you to enter information specific to an application.

Configuring Alert

There are two places to enter configuration information in Alert:

> ➣ Default Configuration Options screens - information entered here will be used for all applications that work with Alert.

> ➣ Custom Configuration screens - information specific to individual Cheyenne Software programs. For example, Custom Configuration allows you to have one Alert setup for InocuLAN, and a different setup for ARCserve. This allows you to tailor the Alerts to the personnel involved with each product.

If InocuLAN is the only application you are using with Alert, you can enter all of your configuration information on the Default Configuration Options screens.

The following section explains how to enter information on the Default Configuration Options screens.

NOTE: You only have to configure Alert on your master server. You do not have to configure Alert on each of your member servers. When a member server sends an alert, it will be sent to the Alert system on your master server.

Default Configuration Options Screens

The information you enter on the Default Configuration Options screens will be used for all applications that work with Alert.

To enter your default Alert configuration:

1. Select Default Configuration from Alert's main menu.

2. Enter information on the Default Configuration Options screen.

You can print up to 70 characters per line at the top of reports and FAXes.

Enter the name of the server where the print queue resides.

Enter the print queue to which trouble tickets will be printed.

Enter the user name Alert should use when logging in.

You can change the password Alert uses when logging in to the print server. The default is <ENTER>.

```
                    Default Configuration Options     Page 1 of 2

Company Name:        SUNNYDALE MANUFACTURING COMPANY
Location:            Roslyn Heights, NY

Trouble Ticket/Facsimile Header
 : *** IMPORTANT NOTIFICATION ***                                      :
 : *** A VIRUS HAS BEEN DETECTED ***                                   :
 :                                                                     :

PRINT server: NY-WRITER
       queue: HPLJ2
    login id:
    password: [Hit Enter To Reset Password]

CENTRAL MODEM server: NY-ENG
               setup:
```

Enter the name of the server with the modem to be used. Use this option to forward alerts to a central modem server.

Enter any unique initialization information required for your modem. The string you enter should only include features unique to your modem or features not normally set during modem initialization. It is recommended that you leave this field blank.

3. Press PAGE DOWN to move to the second screen.

4. Enter information on this screen.

These fields are described on the following pages.

```
                    Default Configuration Options    Page 2 of 2

 BROADCAST recipients:      [Hit Enter To See List]

 MHS          server:       NY-WRITER
       volume:directory     SYS:
              login id:     MAIL
              password:     [Hit Enter To Reset Password]
                  host:     -ASDCDF-
            recipients:     [Hit Enter To See List]

 FAX             host:      NY-TECH_PUB
              login id:     FAX
              password:     [Hit Enter To Reset Password]
            recipients:     [Hit Enter To See List]

    PAGER recipients:       [Hit Enter To See List]
```

5. Press F2 to save your configuration information.

6. Answer **Yes** to confirm.

    You will be brought back to Alert's main menu.

Trouble Tickets

Alert will send a trouble ticket to a designated network printer whenever a virus is discovered.

To configure trouble tickets:

1. Select Default Configuration from Alert's main menu.

You can print up to 70 characters per line at the top of the trouble ticket.

```
                    Default Configuration Options       Page 1 of 2

Company Name:              SUNNYDALE MANUFACTURING COMPANY
Location:                  Roslyn Heights, NY

Trouble Ticket/Facsimile Header
  : *** IMPORTANT NOTIFICATION ***                                      :
  : *** A VIRUS HAS BEEN DETECTED ***                                   :
  :                                                                     :

PRINT server: NY-WRITER
        queue: HPLJ2
     login id:
     password: [Hit Enter To Reset Password]

CENTRAL MODEM server:  NY-ENG
              setup:
```
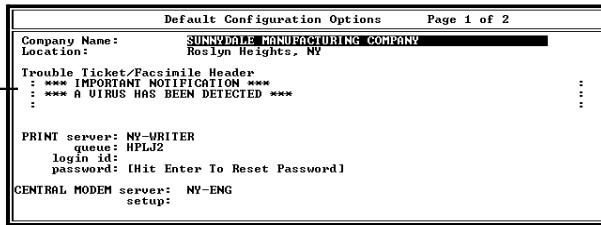
2. Enter a message in the Trouble Ticket/Facsimile Header field to be printed at the top of the trouble ticket.

   The message should indicate that a virus was detected, plus any other information that will help facilitate the recovery process.

3. Enter the name of the print server and print queue.

   For NetWare NDS users, the queue needs a full context name. For example, an NDS print queue name might look like this:

   Q1.CHEYPRNT.SALES.B7

4. Enter a login id and a password, if needed.

   For NetWare NDS users, the login id must be a full context name, and it must log in to the server.

5. Press F2 to save your configuration information.

6. Answer **Yes** to confirm.

Broadcast Recipients

NetWare broadcasts can be sent to specific network
users or groups when InocuLAN detects a virus on your
network.

The following are important notes about broadcasts:

> ➤ If you use Novell's CASTOFF command on
>   a workstation, it will not receive broadcast
>   alerts.

> ➤ For Windows workstations, the WIN.INI file
>   must be modified for broadcasts to be
>   received. Add the following to the LOAD
>   statement: *LOAD=NWPOPUP.EXE*.

> ➤ For Macintosh workstations, copy the Notify
>   Startup Document to each user's Macintosh
>   System folder to receive broadcasts. This
>   document is located on the Novell
>   Macintosh Utilities Distribution Diskette.

When you press ENTER in the *BROADCAST
Recipients* field of the Default Configuration Options
screen, the current list of recipients appears:

*User/Supervisor is
the default
recipient.*

```
┌─────────────────────────────┐
│ Broadcast recipients:       │
│┌───────────────────────────┐│
││USER/SUPERVISOR            ││
│                             │
│                             │
│                             │
│                             │
│                             │
│                             │
│                             │
│                             │
│                             │
│                             │
│└                           ┘│
└─────────────────────────────┘
```
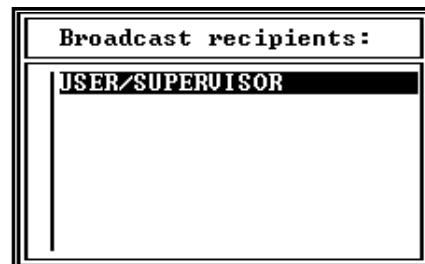
Adding broadcast
recipients

To add broadcast recipients:

1. Press INSERT.

A list of all users and groups not receiving
broadcasts appears:

All of the available
users and groups are
listed. This screen
may look different if
you are using

```
┌─────────────────────────────────┐
│          User List              │
├─────────────────────────────────┤
│ GROUP/EVERYONE                  │
│ USER/ALERT_SUR00438576          │
│ USER/CHEY_USUR                  │
│ USER/ELLEN                      │
│ USER/GUEST                      │
│ USER/KENDALL                    │
│ USER/NAOMI                      │
└─────────────────────────────────┘
```

2. Highlight the user/group you want.

   To select multiple users/groups, press F5 to mark
   each user/group.

3. Press ENTER.

4. Press ESC after you have selected all of the recipients
   you want.

Broadcasts without Alert

You can create an ASCII text file called
NT_USER.DAT (in the InocuLAN home directory on
the server) that InocuLAN will use to broadcast
messages when Alert is not loaded. The InocuLAN
NLM will broadcast to all users defined in this file.
Each line in the file can contain one user name.
NetWare 4.x user names must be distinguished
(complete) names, for example:
ADMIN.ACCNTG.WORK.

Deleting a broadcast recipient

To delete a recipient from the broadcast recipients list:

1. Press ENTER in the Broadcast Recipients field to access
   the User List.

2. Highlight the user/group you wish to delete.

3. Press the DELETE key.

4. Press ESC after you have deleted all of the recipients you want to delete.

MHS Messaging

MHS is the Netware Message Handling System, a collection of Netware NLMs that provide mail delivery service for Netware networks.

The MHS option is used by InocuLAN to send E-mail messages to specific users when a virus is detected. Both NGM Global MHS and Basic MHS are supported. NetWare MHS must be installed on your network in order to be able to send messages.

This section explains the MHS fields on the Default Configuration Options screen. For site-specific details about what to enter in an MHS field, such as Server, contact your Netware administrator.

The MHS fields are described below.

```
                      Default Configuration Options      Page 2 of 2

BROADCAST recipients:      [Hit Enter To See List]

MHS          server:       NY-WRITER
      volume:directory     SYS:
             login id:     MAIL
             password:     [Hit Enter To Reset Password]
                 host:     -ASDCDF-
           recipients:     [Hit Enter To See List]

FAX            host:       NY-TECH_PUB
             login id:     FAX
             password:     [Hit Enter To Reset Password]
           recipients:     [Hit Enter To See List]

   PAGER recipients:       [Hit Enter To See List]
```

Server Name	Enter the name of the server where MHS is installed.
Volume:Directory	Enter the path where MHS is located. Do not enter the actual MHS directory itself. For example, enter `SYS:` not `SYS:MHS`.
Login ID	Enter the user name Alert should use when logging into the MHS server.

Password
Change the password Alert uses when logging in to the MHS server. The default is <ENTER>.

Host Name
Enter the hub name used by the MHS software to identify the server's MHS system.

Recipients
When you press ENTER in the *MHS Recipients* field, the current list of recipients appears:

The recipients list is initially empty.

```
┌──────────────────┐
│ E-Mail Recipients:│
├──────────────────┤
│ │                │
│ │                │
│ │                │
│ │                │
│ │                │
└──────────────────┘
```

Adding MHS recipients
To add MHS recipients, please follow the listed steps.

1. **Press INSERT.**

2. **Enter the E-mail address of the recipient.**

   For NetWare 3.x users, the E-mail address must be in the MHS format: USER@HOST.

   The USER and (MHS) HOST can each consist of up to eight characters separated by the @ symbol.

```
┌─────────────────────┐
│ Enter E-Mail Address │
├─────────────────────┤
│ BOB@-ASDCDF-         │
└─────────────────────┘
```

   For NetWare NDS users, the E-mail address must be in the format: USER@CONTEXT. The address may be up to 512 characters.

3. **Press ENTER.**

4. **Press ESC after you have entered all of the recipients you want.**

SNMP Option

The SNMP option is used to send alerts using an SNMP
(Simple Network Management Protocol) system, such
as NetWare Management System (NMS) and HP Open
View.

To configure SNMP:

1. At the server console, type the following:

   LOAD EDIT SYS:\ETC\TRAPTARG.CFG

   This will open the TRAPTARG.CFG file and allow
   you to enter the necessary information. The file will
   be similar to the following:

```
                     File SYS:\ETC\TRAPTARG.CFG
#############################################################
# traptarg.cfg
#
# Snmp Agent Trap Target (Destination) Configuration
#
# This file specifies all managers that are to receive
# snmp trap messages generated by the Snmp Agent (snmp.nlm)
#
# File Format:
#
# Protocol (name)
#    Specifies the beginning of a list of names or
#    address of managers to which to send traps using the
#    protocol specified by (name) if that protocol is
#    registered as a service provider to the snmp agent.
#
#    All destinations must be preceeded by white space
#    Each destination must be listed on a separate Line
```

2. Enter an IPX address and/or an IP address in the file.

   Under the *Protocol IPX* section, you may enter one
   or more IPX addresses. Under the *Protocol UDP*
   section, you may enter one or more IP addresses.
   Make sure you press the TAB key on the line before
   entering an address.

```
╔══════════════════════════════════════════════════════════════╗
║                  File SYS:\ETC\TRAPTARG.CFG                   ║
╟──────────────────────────────────────────────────────────────╢
║ Protocol IPX                                                  ║
║     # In this section you can put SNMP managers that want to receive║
║     # traps from the local node over IPX.  Managers can be identified║
║     # by NetWare service name (a NetWare file server name, for example)║
║     # or by IPX address.  To specify by IPX address, use the following║
║     # format:                                                 ║
║     #         IPX Network Number: MAC Address                 ║
║     # for example, c9990111:00001B555555                      ║
║     # HP NetServer Assistant                                  ║
║     00000102:0000C0DFC446                                     ║
║ Protocol UDP                                                  ║
║     # In this section you can put SNMP managers that want to receive║
║     # traps from the local node over UDP.  Use either IP address or║
║     # logical name.  (If you use a logical name be sure the name and its║
║     # corresponding ip address appear in the sys:etc\hosts file.)║
║     # By default, the local node sends traps at least to itself.║
║     127.0.0.1        # send traps to the loopback address     ║
╚══════════════════════════════════════════════════════════════╝
```

Enter each IPX address on a separate line here. Be sure to press tab first.

Enter each IP address on a separate line here. Be sure to tab first.

If you enter the same machine under both the IPX Protocol and UDP Protocol sections, you may receive each message twice, depending on the configuration of your network, routers, etc.

3. Press the ESC key to save your entries.

    SNMP entries will not take effect until you down your server and restart it. Be aware that this process will stop all functions and cause all users to be logged out.

Fax Option

The FAX option is used to send a fax when a virus is detected. Cheyenne Software's FAXserve application must be installed on the server being used to send the fax.

This section explains the FAX fields on the Default Configuration Options screen.

The FAX fields are described below.

```
                 Default Configuration Options      Page 2 of 2

BROADCAST recipients:      [Hit Enter To See List]

MHS          server:       NY-WRITER
      volume:directory     SYS:
             login id:     MAIL
             password:     [Hit Enter To Reset Password]
                 host:     -ASDCDF-
           recipients:     [Hit Enter To See List]

FAX              host:     NY-TECH_PUB
             login id:     FAX
             password:     [Hit Enter To Reset Password]
           recipients:     [Hit Enter To See List]

    PAGER recipients:      [Hit Enter To See List]
```

Host Name | Enter the name of the server where FAXserve is installed.

Login ID | Enter the user name Alert should use when logging in to the FAXserve server. If the FAXserve server is loaded in bindery, the login ID must be in bindery format. If FAXserve is loaded as NDS, the login ID must be in NDS format, and must be something *other than* "supervisor."

Password | Change the password Alert uses when logging in to the FAXserve server. The default is <ENTER>.

Recipients

When you press ENTER in the *FAX Recipients* field, the current list of recipients appears:

The list is initially empty.

```
┌─────────────────────────────┐
│      Fax Phone Numbers       │
├─────────────────────────────┤
│ │                            │
│ │                            │
│ │                            │
│ │                            │
│ │                            │
│ │                            │
└─────────────────────────────┘
```

Adding FAX
recipients

To add FAX recipients:

1. Press INSERT.

2. Enter the FAX parameters.

```
┌──────────────────────────────────────────────────────┐
│                    Fax Parameters                      │
├──────────────────────────────────────────────────────┤
│              Title : REBECCA_SMITH                     │
│         FAX Number : 6258838                           │
│ Fax Cover Page File :                                  │
│                                                        │
└──────────────────────────────────────────────────────┘
```

Enter the name of the person to whom you are sending the fax.

FAX Number

Enter the fax number of the recipient.

Fax Cover Page File

Enter the path for the file that contains the cover sheet to use with this fax. This file must be on a FAXserve server and it must be a .PCX file. Refer to your FAXserve documentation for more information.

3. Press ESC when you are done.

Pager Recipients

The pager option is used to a send a pager message when a virus is detected. The pager can be numeric or alphanumeric.

The *PAGER recipients* field is located on the Default Configuration Options screen:

```
                  Default Configuration Options      Page 2 of 2
BROADCAST recipients:      [Hit Enter To See List]

MHS        server:         NY-WRITER
      volume:directory     SYS:
           login id:       MAIL
           password:       [Hit Enter To Reset Password]
               host:       -ASDCDF-
         recipients:       [Hit Enter To See List]

FAX          host:         NY-TECH_PUB
           login id:       FAX
           password:       [Hit Enter To Reset Password]
         recipients:       [Hit Enter To See List]

        PAGER recipients:  [Hit Enter To See List]
```

The PAGER recipients field.
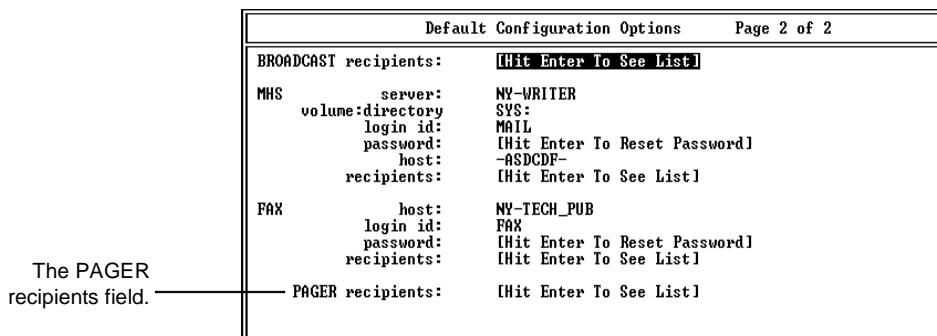
When you press ENTER in the *PAGER recipients* field, the current list of recipients appears:

The list is initially empty.

```
              Pager Recipients



```
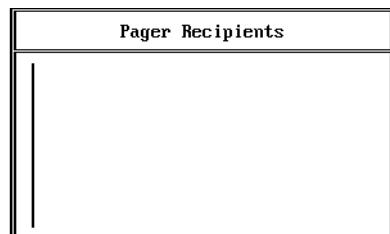
Adding pager recipients

To add pager recipients:

1. Press INSERT.

The Communications Configuration screen appears:

2. Enter information on the Communications Configuration screen.

```
┌─────────────────────────────────────────────────┐
│            Communications Configuration           │
├─────────────────────────────────────────────────┤
│            Pager Type: Numeric Pager              │
│          Pager Number:                            │
│              Pager ID:                            │
│             Baud Rate: 1200                       │
│               Site ID:                            │
│       Connection Delay:                           │
│         Message Delay:                            │
│             Data Bits: 0                          │
│                Parity: None                       │
│             Stop Bits: 0                          │
│                                                   │
│                                                   │
└─────────────────────────────────────────────────┘
```
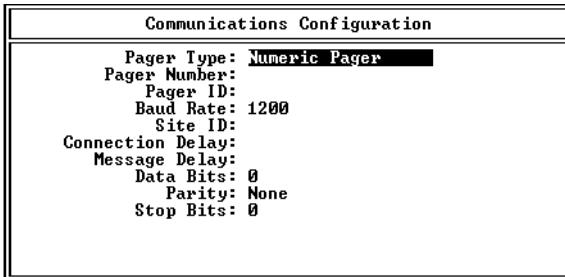
Pager Type	Indicate if you are using a numeric or alphanumeric pager. Press ENTER to select a pager type.
Pager Number	Enter a maximum of 24 characters. If a digit, such as 9, must be dialed to get a dial tone, it must be included in this field.
	A comma can be entered to indicate a one second pause. If a longer pause is desired, a string of commas can be entered.
	A dash (-) can be used to separate digits, but it has no function. (Since this can vary by modem, you should verify this with your modem manual.)
Pager ID	Enter up to eight digits to identify the pager that will receive the alerts.
Baud Rate	Indicate the baud rate being used by your modem. Press ENTER to display a list of baud rates from which to choose.
Site ID	Enter up to four digits to identify where the alert occurred. This number is included in the message to the pager. Therefore, if the number is less than four digits, you should use leading zeros.

Connection Delay	This field applies only to numeric pages. Enter one or more commas (,) to delay the connection with the pager company. Typically, a comma represents a one second pause. However, this may vary by brand of modem. Check your modem guide for more information.
	When a phone number is dialed, a connection is made. The connection may be established immediately or it may be delayed. This will vary with your pager company, location, time of day, telephone equipment, and telephone traffic. If the connection is not established immediately, adding a delay can prevent the alert from being sent before the connection is established.
Message Delay	This field applies only to numeric pages. Enter one or more commas (,) to indicate the time to wait between the connection being made and the alert message being sent. Typically, a comma represents a one second pause. However, this may vary by brand of modem. Check your modem guide for more information.
Data Bits	Enter the number of data bits, 7 or 8, that your modem uses. *
Parity	Indicate the parity setting, none, odd, or even, of your modem. Press ENTER to display a list of parity settings from which to choose.
Stop Bits	Enter the number of stop bits, 1 or 2, that your modem uses. *

Recommended settings

Following are recommended pager settings:

Numeric pager	Alphanumeric pager
Baud = 1200	Baud = 300 or 1200
Connection delay = 3 to 4	No connection delay
Message delay = 3 to 4	No message delay
8 data bits, no parity, 1 stop bit	7 data bits, even parity, 1 stop bit

3. **Press ESC to save your information.**

4. **Answer Yes to confirm.**

Interpreting the Pager Message

Numeric pagers

When a numeric pager is sent a virus alert, the coded message will appear as: **Message = DDSSSSCC**

DD is the virus detection code number. It tells you which component of InocuLAN has detected a virus.

You must check InocuLAN's scanning records to determine which workstation or file server is infected and which files or directories contain the virus.

Virus Detection Code	Description
01	IMMUNE detected viral activity on a workstation. Viral activity includes: Unauthorized reformatting of the hard disk, a change in the boot sector, or a change in the partition table.
02	IMMUNE detected a virus in a workstation file.
03	A boot virus or a change to the Critical Disk Area was detected on a workstation by the Run Scanner option.
04	The InocuLAN Manager detected a virus at a workstation. The file containing the virus will be handled according to the action chosen in the "Action Upon Detection Field" on the Run Scanner form.
05	The InocuLAN Schedule Scanner detected a virus on the file server. The file containing the virus will be handled according to the action chosen in the "Action Upon Detection Field" on the Schedule Server Scanning Form.
06	The Real-time Monitor detected a virus on a server. The file containing the virus will be handled according to the action chosen in the "Action Upon Detection Field" on the Real-time Server Monitor Form.

Virus Detection Code	Description
07	IMMUNE detected a virus in memory.
08	IMMUNE detected a boot virus.
10	The Macintosh scanner detected a virus on a Macintosh workstation.
11	The Macintosh INIT detected a virus on a Macintosh workstation.

SSSS is the user defined site number from the Pager and Modem Specifications form. The site number represents the server that sent the Alert.

CC is the user defined custom code from the Pager Parameters form. The custom code represents the server that sent the message.

Alphanumeric pagers

There are several messages that can be sent to an alphanumeric pager. Each message is listed below. Words that appear in italics are variables that will be filled in with an actual user name, workstation address, path and file name, virus name, or server name.

IMMUNE Detected Viral Behavior - username at workstation address

IMMUNE Detected a Virus in [path] - username at workstation address

Boot Virus Detected - username at workstation address

Manager Detected a Virus [virusname] in [path] - username at workstation address

Infected File [servername/path] Detected

Infected File [path*] Accessed by username at workstation address

* This can be the path on a server or workstation.

Custom Configuration Screens

The Custom Configuration screens are used to enter information specific to individual Cheyenne Software programs. For example, Custom Configuration allows you to have one Alert setup for InocuLAN, and a different setup for ARCserve. This allows you to tailor the Alerts to the personnel involved with each product.

If InocuLAN is the only application you are using with Alert, you can enter all of your configuration information on the Default Configuration screens.

To enter your InocuLAN-specific configuration:

1. Select Custom Configuration from Alert's main menu.

2. Select InocuLAN.

   All of the available options are listed.

3. Select an option.

4. Set the Enable Custom Configuration field to YES.

5. Enter information specifically for InocuLAN.

   Refer to the section 'The Default Configuration Options screen' for information about specific fields.

Port Configuration

When you select *Port Configuration*, the following menu appears:

```
┌─────────────────────────────┐
│     Port Configuration      │
├─────────────────────────────┤
│ Attach Modem To Port        │
│ Detach Modem From Port      │
│ Reset Modem                 │
└─────────────────────────────┘
```
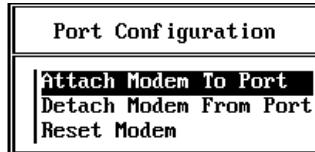
Attach Modem To Port

You use this option the first time you are configuring Alert or if your modem was off when Alert was loaded.

To use this option:

1. Select Attach Modem To Port.

2. Select a port from the window that appears.

```
┌─────────────────────────────┐
│        Select Port          │
├─────────────────────────────┤
│ Board #0/Port #0            │
│                             │
│                             │
│                             │
└─────────────────────────────┘
```
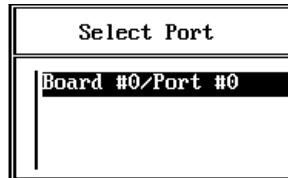
You use this option to detach a modem, for example, because it was not working properly.

To use this option:

1. Select Detach Modem From Port.

2. Select a port from the window that appears.

Resetting the modem   Your modem is automatically reset when Alert is
                      loaded. You could use this option for a modem
                      problem, such as a communication that did not end
                      properly and locked your modem. To use this option:

1.   Select Reset Modem.

Alert's Messages Report Log

Every message that is generated by Alert is stored in the Messages Report Log. You can view, print, or clear this log.

Displaying the
Messages Report
Log

To display the Messages Report Log:

1. Select Messages Report Log from Alert's main menu.

Your Messages Report Log, similar to the one listed below, will appear:

*You are initially
taken to the end of
the file where the
most recent
messages appear.*

```
                      Alert Message Report Log
10-29-95 11:55:20 INOCULAN: Message For Snmp Priority Red:
10-29-95 11:55:20 10/29 11:55 Infected File [SUNNY/SYS:\PUBLIC\ADSG.COM] Acces
10-29-95 12:11:50 INOCULAN: Message For Fax Priority Red:
10-29-95 12:11:50 10/29 12:11 Infected File [SUNNY/SYS:\PUBLIC\ADSG.COM] Acces
```
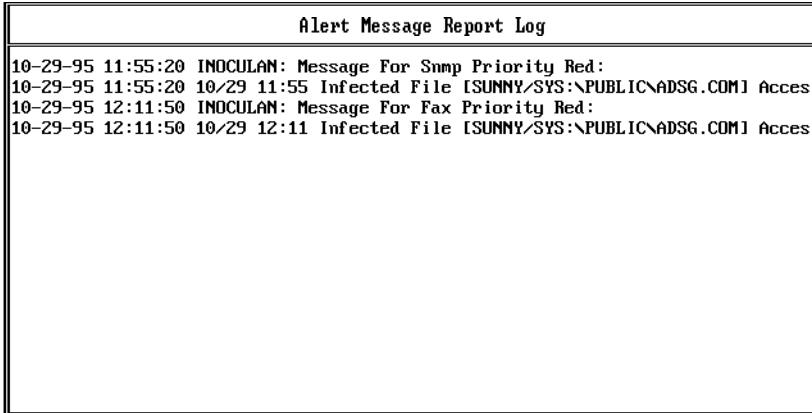
Printing the
Messages Report
Log

You can print the Messages Report Log to the server's print queue.

To do this:

1. Press F3.

Clearing the
Messages Report
Log

You can delete the Messages Report Log. You might want to do this if Alert has been running for a long time and the log has grown large.

To clear the log:

1.   Press F4.

Alert's Activity Log

While the current status of Alert is displayed on Alert's main menu, a historical listing is stored in the Activity Log. You can view, print, or clear this log.

Displaying the Activity Log

To display the Activity Log:

1. Select Activity Log from Alert's main menu.

Your Activity Log, similar to the one listed below, will appear:

You are initially taken to the end of the file where the most recent messages

```
                        Alert Activity Log
09-20-95 11:29:57 Shutting Down Alert Server
09-20-95 12:34:11 Server Attached
09-20-95 12:34:11 Asynchronous AIO Drivers Not Loaded
09-20-95 12:34:22 Shutting Down Alert Server
09-20-95 12:39:26 Server Attached
09-20-95 12:39:26 Asynchronous AIO Drivers Not Loaded
09-20-95 12:39:28 Servicing Alert 0
09-20-95 12:39:28 Starting Fax Send
09-20-95 12:39:30    Fax Sent To Ellen
```

Printing the Activity Log

You can print the Activity Log to the server's print queue.

To do this:

1. Press F3.

Clearing the Activity Log

You can delete the Activity Log. You might want to do this if Alert has been running for a long time and the log has grown large.

To clear the log:

1. Press F4.

COMMAND LINE OPERATION

You can run InocuLAN from a DOS prompt. This enables you to scan your network without running the InocuLAN Manager. You can also initiate InocuLAN scans from a batch file or login script.

In this chapter, you will learn:

Running InocuLAN From the Command Line

You can run InocuLAN from a workstation DOS prompt. This allows you to scan your network without running the InocuLAN Manager. The command (and any options) you use to run InocuLAN can be used in batch files and login scripts to initiate InocuLAN scans.

Command line InocuLAN uses less memory

When you run InocuLAN from the command line, InocuLAN uses a program called INOCUCMD.EXE to execute scanning jobs. This program uses about 100K less memory than InocuLAN (approximately 410K for INOCUCMD.EXE vs. 510K for InocuLAN).

Command line operation uses the commands INOCULAN and INOCUCMD interchangeably.

Memory is checked when you run InocuLAN

InocuLAN checks for memory-resident viruses in RAM from 0 to 640 kilobytes each time InocuLAN is executed from the command line. If a virus is detected, InocuLAN will neutralize it.

The Critical Disk Area is also scanned. Boot viruses are cured, if possible. If not, you will be notified by a screen message.

Running InocuLAN without options

You can run InocuLAN by doing the following:

1. Type INOCULAN source at a DOS prompt.

If necessary, specify the path where InocuLAN is located.

Source is the path to scan. You can enter any of the following:

Source	What will be scanned
*	All local hard drives.
drive:\	The entire drive, including all directories, subdirectories, and files will be scanned. Mapped drive specifications can be used. For example, to scan your C drive, you would enter: INOCULAN C:\
drive:\directory	All subdirectories and files in the stated directory will be scanned. For example, to scan all the files in your DOS directory, you would enter: INOCULAN C:\DOS
server	The entire server, including all volumes, directories, subdirectories, and files will be scanned. For example, to scan a server named PAYROLL, you would enter: INOCULAN PAYROLL
server/vol:	All directories, subdirectories, and files on this volume will be scanned. For example, to scan the APRIL volume on the PAYROLL server, you would enter: INOCULAN PAYROLL/APRIL:
file	Only the file you specify will be scanned. A full path is required. For example, to scan the WS.BAT file in your DOS directory on your C drive, you would enter: INOCULAN C:\DOS\WS.BAT

InocuLAN's options

There are several options you can use at the command line.

To run InocuLAN with options:

1. Type **INOCULAN *source option*** at a DOS prompt.

    You can specify one or more options. Options must be separated with a space and can be entered using a leading slash (/), dash (-), or space. For example, both of the following would produce the same results:

    INOCULAN C:\   /EXE   /SEC

    INOCULAN C:\   EXE   SEC

    The **option** choices are explained below, by category.

    What to scan

Option	Description
EXA	Detects boot viruses only.
EXE	Scan executable files only. This includes, but is not limited to: *.EXE, *.COM, *.OVL, *.PRG, *.APP, *.SYS, *.DRV, and *.OVR.
NOC	Skips compressed files. By default, InocuLAN will scan compressed files of the .ZIP and .ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.)
NCD	This option will cause InocuLAN to avoid scanning CD-ROM drives on your workstation. It will not skip CD-ROM drives on servers.
NOS	Does not scan subdirectories under the source directory.
UPM	Scans memory up to 1M for viruses.

Scan method

Option	Description
FST	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* Executable files (*.EXE, *.COM, etc.) are always fully scanned.
NS	Non-stop. Normally, you can stop a scan by pressing the ESC key. The NS option will disable the ESC key.
SEC	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
REV	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when you have not selected an scanner Action from the list below. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Action upon virus detection

Option	Description
DEL	Deletes an infected file from your workstation.
CUR	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to /REN below). Even if InocuLAN cures the file, we recommend you purge the infected file and then restore the original file.

Option	Description
REN	Renames infected files by giving them an extension of .AVB. Files with this extension will not be scanned.

If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0. |
MOV	Moves an infected file from its current directory to the INOCULAN\VIRUS directory.
PUR	Deletes an infected file so that it cannot be recovered (for example, using the DOS UNDELETE command).
M&R	Renames infected files by giving them an .AVB extension and then moves them to the INOCULAN\VIRUS directory.

NOTE: If a virus is found in a compressed file, it will only be reported. Other scans actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

Help option

Option	Description
HEL or ?	Displays help menu.

Reporting options

Option	Description
LIS <report file path & name>	Generates a scanning report file using the specified path name. For example: LIS C:\INOCULAN\REPT.TXT
APP	Appends the scanning report to any previously created scanning reports.

Critical Disk Area options

Option	Description
BAK <destination path>	Backs up the Critical Disk Area to the file specified in the path.
RES <source path>	Restores the Critical Disk Area using the source file specified in the path.
EXM <backup path>	Examines the Critical Disk Area. To compare to previously backed up version, enter a backup path where it can be found.

Command line return codes

For use with batch file processing, the following return codes apply to the command line scanner:

Error level	Meaning
Greater than 100	A virus was detected.
Greater than 2	Some kind of failure to scan.
1	A user pressed the escape key to exit the scan.
0	The scan was successful. No viruses were detected.

Sample batch file

```
@echo off

inocucmd %1 %2 %3 %4 %5 %6 %7 %8

if errorlevel 100 goto virus

if errorlevel 2 goto failure

if errorlevel 1 goto user_escape

goto no_problem

:virus

echo virus detected

goto done

:failure

echo scan failed for some reason

goto done

:user_escape

echo user hit escape

goto done

:no_problem

echo scan completed successfully

:done
```

6

C h a p t e r

USING THE INOCULAN SERVER

While most administrators will manage operations from their workstation, there are several InocuLAN functions you can perform directly from the file server console.

In this chapter, you will learn:

Loading InocuLAN

Before using the InocuLAN console, you must load InocuLAN on your server.

<table>
<tr><td>

Note for users of memory checking NLMs

</td><td>

If you have a memory-checking NLM loaded on your server (such as Nu-Mega Technologies' NETcheck and Novell's Protect), you must unload it before loading the InocuLAN NLM. The order of loading is important, and the InocuLAN NLM must be loaded first. (When unloading InocuLAN, the order is also important. These NLMs must be unloaded before you unload the InocuLAN NLM.)

If you are loading NETcheck or Protect from the AUTOEXEC.NCF, the following guidelines explain your options for loading InocuLAN from the AUTOEXEC.NCF.

</td></tr>
</table>

> ➤ If you have multiple volumes, load InocuLAN before mounting the other volumes.
> ➤ If SYS: is your only volume, it is best not to load InocuLAN from the AUTOEXEC.NCF.

<table>
<tr><td>

Load the InocuLAN Server

</td><td>

To load the InocuLAN Server without any options:

1. Type `LOAD INOCULAN` at the file server console.

The InocuLAN NLM is loaded with its default settings.

To load the InocuLAN Server with options:

1. Type `LOAD INOCULAN` *options* at the file server console.

</td></tr>
</table>

The options you can use are described in the following table:

Option	Description
AUTOUPDATE	Enables the Signature AUTO update feature. When enabled, auto-update automatically synchronizes all of your InocuLAN domain servers with the most current version of InocuLAN's virus signature files. The default value is off.
DEL_DOM	Deletes the server from its domain. It is recommended that you use the Domain Manager for deleting a domain.
DOMUPDATE=n	Specifies the time that passes between each update of domain information. The default value is 3,600 seconds (1 hour).
DOS_ONLY	Scans only DOS and Windows files. Macintosh files are not scanned. This is not a default value.
GRACE=n (n=seconds)	Changes the grace period for Enforcement. The grace period is the amount of time the user has to load IMMUNE before being disconnected from a server. The default grace period is 60 seconds. (Messages are sent to the user informing him or her to load IMMUNE during the grace period.) The number of seconds must be in 30 second intervals (such as 30, 90, or 120).
HELP	Displays a summary of all available options.
INACTIVE	Loads InocuLAN in an inactive state. InocuLAN can be activated later either through the server console or the Domain Manager in DOS or Windows. This is not a default value.

Option	Description
KTIME=n	The number of milliseconds InocuLAN will wait before scanning files copied to the server with the NCOPY command or other applications that behave similarly. The default value is 0.
NOLOCAL	Disables alert notification. If the notification system is disabled and a virus is detected by one of the domain server scanners, a message will not be generated. However, a record of the virus and any action taken will appear in the Activity Log. This is not a default value.
NOLOGIN	Disables the Enforcement feature. This is not a default value.
SETENFORCE	Activates Enforcement for the servers. (The master server can override this setting.) Enforcement is off by default.

After loading InocuLAN, the console screen appears:

```
InocuLAN  V4.0  (1000 user)                    NetWare Loadable Module

InocuLAN Server Up Time: 0 Day  4 Hours  36 Minutes  21 Seconds
            Domain Name: DOMAIN-ZED
     Master Server Name: NY-SUNNY
        Real-time Scan: Incoming/Outgoing Files
    Last Virus Detected:
       Last Virus File:
  Incoming Files Scanned:        0          Viruses Found:        0
  Outgoing Files Scanned:        0          Viruses Found:        0


                        Available Options
                      Deactivate InocuLAN
                      Job Queue Operation
                      Configuration
                      View Activity Log
                      Lock Screen
                      Exit
                 <F1>:Help    <Enter>:Select
```

Accessing the InocuLAN Menu

The InocuLAN Server NLM runs on a file server. From this server, there are several InocuLAN functions you can run.

To access the InocuLAN menu on the server:

1. Press CTRL and ESC together.

   The server's list of current screens will be displayed.

2. Select InocuLAN Console

   InocuLAN's Available Options menu will appear:

   ```
   ╔════════════════════════╗
   ║   Available Options    ║
   ╠════════════════════════╣
   ║ Deactivate InocuLAN    ║
   ║ Job Queue Operation    ║
   ║ Configuration          ║
   ║ View Activity Log      ║
   ║ Lock Screen            ║
   ║ Exit                   ║
   ╚════════════════════════╝
   ```
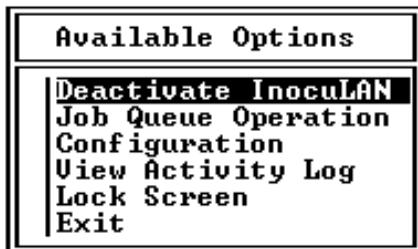
   Each of these options is described on the following pages.

Activating/Deactivating InocuLAN

Activating the InocuLAN Server enables background operations, such as scanning.

Deactivating InocuLAN suspends all scanning operations. While InocuLAN is deactivated, <u>only</u> Notification is still operational. You can still schedule scans, but none will be performed.

NOTE: When you deactivate/activate InocuLAN on your master server, InocuLAN will be deactivated/activated on all of its member servers. If this option is used on a member server, the domain configuration settings will eventually overwrite this member server's configuration settings.

Job Queue Operation

This option lets you perform an immediate scan of your domain server and to view the status of an active job, a completed job or a scheduled job.

Performing an immediate scan

To perform an immediate scan:

1. **Choose Job Queue Operation from the Available Options menu.**

   The Job Queue screen appears:

```
 InocuLAN  V4.0  (1000 user)                      NetWare Loadable Module
┌──────────────────────────────────────────────────────────────────────┐
│ InocuLAN Server Up Time: 0 Day  3 Hours  34 Minutes  32 Seconds        │
│            Domain Name: DOMAIN-1                                        │
│      Master Server Name: NY-SUNNY                                       │
│          Real-time Scan: Incoming and Outgoing Files                   │
│     Last Virus Detected:                                               │
│         Last Virus File:                                               │
│   Incoming Files Scanned:           0            Viruses Found:       0 │
│   Outgoing Files Scanned:           0            Viruses Found:       0 │
└──────────────────────────────────────────────────────────────────────┘
┌──────────────────────────────────────────────────────────────────────┐
│ Status   Execution Time   Owner     Source                     Action  │
│ ┌────────────────────────────────────────────────────────────────────┐│
│ │DONE     Sep 18 12:39    Console   SYS:\NORTON               Report  ││
│ │DONE     Sep 18 12:45    Console   SYS:\ACCESS               Report  ││
│ │DONE     Sep 18 12:46    Console   SYS:                      Report  ││
│ │READY    Sep 18 13:20    Local     *                         Report  ││
│ │READY    Sep 18 13:21              SYS:                      Report  ││
│ │                                                                    ││
│ └────────────────────────────────────────────────────────────────────┘│
└──────────────────────────────────────────────────────────────────────┘
      <F1>:Help  <F3>:Insert  <Del>:Delete  <Enter>:Modify  <Esc>:Exit
```

General InocuLAN information is shown here.

InocuLAN status information is shown here.

2. **Press INSERT to bring up the Immediate Server Scanning Form.**

```
┌──────────────────────────────────────────────────────────────┐
│              Immediate Server Scanning Form                    │
│ ┌──────────────────────────────────────────────────────────┐ │
│ Source Directory: ████████████████████████████████████████   │
│                                                                │
│ Traverse Directory:    Yes    Delay If CPU Utilization Up To 99 %│
│                                                                │
│ File Selection: <Press ENTER To Select>    Scan Type:   Secure │
│                                                                │
│ Repeat Interval:  0 Months  0 Days  0 Hours  0  Minutes        │
│                                                                │
│ Action Upon Virus Detection: Report Only                       │
│                                                                │
│ Scan Compressed Files: Yes          Skip Netware Compressed: Yes│
└──────────────────────────────────────────────────────────────┘
```

3. **Enter information on the Immediate Server Scanning Form.**

Source Directory	Enter the directory where scanning should start. You can select the entire server, a specific volume, or a specific directory or subdirectory.
	Press **INSERT** to display available volumes and directories or enter an asterisk (*****) to scan the entire server.
	Press **ESC** when done.
Traverse Directory	Enter Yes to scan all subdirectories under the source directory or No to scan only the source directory. For example, if you answer No and an entire server volume is selected as the source directory, only its root will be scanned.
Delay If CPU Utilization Up To %	Enter a CPU Utilization percentage to indicate the point at which InocuLAN scanning should slow down. (CPU Utilization represents the percentage of time the file server CPU is being used.)
	Press **ENTER** to select specific types of DOS and Macintosh files for scanning.
	For *DOS files*, you can select all files or a selection of executable files. If you select *EXECUTABLE FILES*, you can further define which files to scan by their extensions.
	For *Macintosh files*, you can select all files, application type files, or files with a resource fork (the portion of a Macintosh disk file that contains the program code, font information, and other data not normally generated by a user). You can also choose not to scan Macintosh files.
	Press ESC when done.

Scan Type

Select one of the following Scan Types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* Executable of files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Repeat Interval

If you want to scan only one time, these fields should be set to zero. If the file server scanning is to be repeated automatically, enter the time interval between each scanning.

Action Upon Virus Detection

Press **ENTER** to display a list of options. Regardless of which option you choose, a message will appear in the scanning report when a virus is detected.

Action	Description
Report Only	Displays a message on the screen.
Delete File	Deletes an infected file from the server.

Action	Description
Rename File	Renames infected files by giving them an .AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners (except the Real-time Monitor). (See the note about Macintosh files below.)
	If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB, and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with a .AVB extension (refer to 'Rename File' above).
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory. (See the note below for Macintosh files.)
Purge File	Deletes an infected file so that it cannot be recovered.
Move and Rename File	Renames infected files by giving them an .AVB extension and then moves them to the INOCULAN\VIRUS directory. (See the note below for Macintosh files.)

NOTE: If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

An infected Macintosh file cannot be renamed or moved.

Every Macintosh file has a file type. If a virus is found, the file type is changed to prevent the file from being used and prevent the virus from spreading. The file types are:

Macintosh File Type	New File Type
Application - APPL	INOA
Data - DATA	INOD
Resources - RSRC	INOR
Stack - STAK	INOS
Text - TEXT	INOT

Scan Compressed Files

Select this option for InocuLAN to scan compressed files. By default, InocuLAN scans files of the ZIP and ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, click the Add button.

Skip Netware Compressed Volume

This option will cause InocuLAN to avoid scanning any NetWare compressed files on your servers. This is the default value. Scanning compressed files will increase the scanning time.

4. When done, press F2 to begin the scan.

Server Status information

The Job Queue screen shows status information for InocuLAN jobs.

```
 Status  #  Execution Time Owner        Source                Action
┌────────────────────────────────────────────────────────────────────┐
│READY    3 Nov 26 15:16  Console      SYS:\HPSERVER          Report  │
│DONE     2 Nov 26 15:15  Console      SYS:\SYSTEM            Rename  │
│DONE     1 Nov 26 15:14  Console      SYS:\MAIL\16010022     Report  │
│                                                                      │
│                                                                      │
│                                                                      │
└────────────────────────────────────────────────────────────────────┘
```

Job status is
reported
here.

For detailed information on a job, highlight the job and press ENTER or F3. For an active job, the job progress will be shown, as below:

Field information is updated as the job proceeds, and the Progress bar shows what percentage of the scan has completed.

```
┌────────────────────────────────────────────────────────────────────┐
│                    Immediate Server Scanning                         │
│            Client: Console Operator                                  │
│  Scan   DOS File: SYS:\ACCESS\INSTALL\MSAJU100.DL$                   │
│             Size: 38,945                                             │
│    Infected Files: 0                                                 │
│     Viruses Found: 0                                                 │
│  Files   Scanned: 94                                                 │
│  KBytes Scanned: 17,613                                              │
│                                                                      │
│         Progress: ▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓░░░░    81 %             │
└────────────────────────────────────────────────────────────────────┘
```
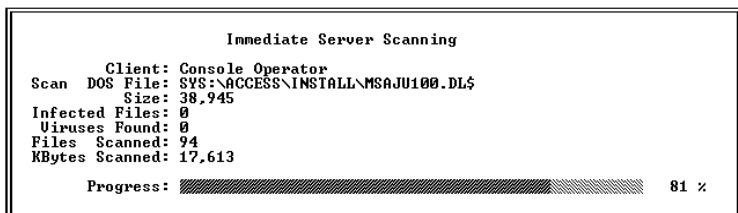
Terminating an
active job

To terminate an active scanning job:

1. Highlight the active job and press ENTER.

2. With the active job window open, press F4.

3. Answer `Yes` to confirm.

Configurations

There are five different options available under *Configuration*:

- ➢ Activate/Deactivate Enforcement
- ➢ Real-time Monitor
- ➢ Update Virus Signature
- ➢ Enable/Disable Signature Files AUTO Update
- ➢ NLM Information

Activate/Deactivate Enforcement

When Enforcement is active, users must load WIMMUNE (in Windows) or IMMUNE (in DOS), or access to the InocuLAN domain server will be denied. See "Using Enforcement" in Chapter 5 for more information.

Real-time Monitor

The Real-time Monitor scans files on a domain server in real-time. Files can be scanned on an incoming or outgoing basis, or both. When you select *Real-time Monitor* from the Configuration Menu, the Real-time Configuration Form appears:

```
╔══════════════════════════════════════════════════╗
║              Real-time Configuration Form           ║
║ ┌───────────────────────────────────────────────┐ ║
║ Direction:       Incoming and Outgoing Files        ║
║                                                     ║
║ File Selection: <Press ENTER To Select>   Scan Type:   Secure ║
║                                                     ║
║ Action Upon Virus Detection:Broadcast               ║
║ └───────────────────────────────────────────────┘ ║
╚══════════════════════════════════════════════════╝
```

The Real-time Monitor does not scan compressed files.

Press ENTER to display a list of options.

Option	Description
Incoming files	Files being copied to the domain server and files being opened for writing on the server are *incoming* files. Incoming files are scanned after the file is closed.
Outgoing files	Files being copied from the server and files that are being executed from the server are *outgoing* files. Outgoing files are scanned when the file is opened. If the file is found to be infected, users will be denied access to it.
Incoming/ Outgoing Files	Scans incoming files and outgoing files.
Disabled	Disables the Real-time Monitor.

Scan Type   Select one of the following Scan Types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* This option only applies to files. Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.

Scan Type	Description
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

File Selection

Press ENTER to select specific types of DOS and Macintosh files for scanning.

For *DOS files*, you can select all files or a selection of executable files. If you select executable files only, you can further define which files to scan by their extensions.

For *Macintosh files*, you can select all files or just application type files or files with a resource fork (the portion of a Macintosh disk file that contains the program code, font information, and other data not normally generated by a user). You can also choose not to scan Macintosh files.

Action Upon Virus Detection

Press ENTER to display a list of options. Regardless of which option you choose, a message will appear in the Activity Log when a virus is detected.

Action	Description
Report Only	Displays a message on the bottom of the screen.
Delete File	Deletes an infected file from the server.

Action	Description
Rename File	Renames infected files by giving them an .AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners (except the Real-time Monitor). If you enter a different extension, these files will be scanned by InocuLAN's scanners. (See the note about Macintosh files below.) If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB, and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory. (See the note below for Macintosh files.)
Purge File	Deletes an infected file so that it cannot be recovered.
Move & Rename File	Renames infected files by giving them a different extension and then moves them to the INOCULAN\VIRUS directory. (See the note below for Macintosh files.)

An infected Macintosh file cannot be renamed or moved.

Every Macintosh file has a file type. If a virus is found, the file type is changed to prevent the file from being used and prevent the virus from spreading. The file types are:

Macintosh File Type	New File Type
Application - APPL	INOA

Macintosh File Type	New File Type
Data - DATA	INOD
Resources - RSRC	INOR
Stack - STAK	INOS
Text - TEXT	INOT

Update Virus Signature

This option allows you to update your virus signature file without having to unload InocuLAN. If you want to use this option, you must make sure the new signature file, VIRSIG.DAT, is in your InocuLAN directory.

Enable/Disable Signature Files AUTO Update

When this option is enabled, InocuLAN will automatically synchronize all of your InocuLAN domain servers with the most current version of InocuLAN's virus signature files (VIRSIG.DAT, INMEM.DAT, and VIRUS.LST).

NLM Information

This option provides information on various aspects of InocuLAN.

```
NLM Information
               Serial Number:  4DZΩ337
        Signature File Version:  3.10
          Signature File Date:  11/14/95
               Engine Version:  3.10
                  Engine Date:  11/15/95
      Enforcement Grace Period:  60 seconds
     Send Alert To Local Server:  Yes
                  NCOPY Delay:  0 ms
         Domain Update Interval:  600 seconds
```

Serial Number	Displays your InocuLAN serial number.
Signature File Version/Date	Indicates the version and date of the virus signature file being used.
Engine Version/Date	Indicates the version number and date of the InocuLAN engine being used.
Enforcement Grace Period	Indicates the amount of time a user has to load WIMMUNE or IMMUNE before being disconnected from the server. This value is set through the Domain Manager. See 'Using Enforcement' in Chapter 3 for details.
Send Alert to Local Server	YES indicates that a domain member will handle alerts along with the Master Server. This is configured from the Domain Manager or using the load option NOLOCAL.
NCOPY delay	The number of milliseconds InocuLAN will wait before scanning files copied to the server with the NCOPY command or other applications that behave similarly. The default value is 0.
Domain Update Interval	Specifies the time that passes between each update of domain information. This value is set through the Domain Manager or when loading InocuLAN.

Viewing the Activity Log

The Activity Log contains information about the operations performed by InocuLAN. The log tells you when:

> ➤ InocuLAN is loaded on your server.
> ➤ A virus is discovered by IMMUNE or the Real-time Monitor. (Viruses detected by the Workstation, Domain, Run, or Schedule Server Scanners are reported in the Scanning Report.)
> ➤ The server's virus signature file is updated.

Although each InocuLAN domain server has its own Activity Log, the master server's Activity Log will report information about viruses discovered by IMMUNE or the Real-time Monitor on member servers.

NOTE: This is the same Activity Log that you can view from the InocuLAN for DOS and InocuLAN for Windows Managers.

To view the Activity Log:

1. Choose View Activity Log from the menu.

    The Activity Log appears:

```
                              Activity Log
INFO   Nov 19 13:24   InocuLAN Server is Ready
WARN   Nov 19 13:27   Enforcement Activated by Console
CRIT   Nov 19 14:25   Real-time Configuration: Checking: Incoming/Outgoing Fil
INFO   Nov 19 14:25   InocuLAN Server is Ready
WARN   Nov 19 14:26   Enforcement Activated by Console
WARN   Nov 19 14:27   Enforcement Deactivated by Console
WARN   Nov 19 14:27   Enforcement Activated by Console
CRIT   Nov 19 14:29   Real-time Configuration: Checking: Incoming/Outgoing Fil
INFO   Nov 19 14:29   InocuLAN Server is Ready
WARN   Nov 19 14:29   Enforcement Activated by Console
CRIT   Nov 19 14:30   Boot Virus Detected -   at 435c494e-4e4fb1000011
CRIT   Nov 19 14:30   Send Alert NPAGER Code 03
CRIT   Nov 19 14:57   Real-time Configuration: Checking: Incoming/Outgoing Fil
CRIT   Nov 19 15:02   SCAN: [NY-SUNNY/Job #0] Detected Infected File(s). See S
CRIT   Nov 19 15:02   Send Alert NPAGER Code 05
CRIT   Nov 19 16:07   Real-time Configuration: Checking: Incoming/Outgoing Fil
CRIT   Nov 24 12:59   Real-time Configuration: Checking: Incoming/Outgoing Fil
```

The message severity level is indicated in the first column.

Message severity level

There are three severity levels for Activity Log messages, explained below:

Message Type	Description
Critical Message - CRIT	This is the highest level message. It requires your immediate attention once logged. This message could mean, for example, that a virus was detected, or there is a critical problem on the network. This is the default.
Warning Message - WARN	The second priority message tells you if InocuLAN skips a file, and other non-critical information.
Informational Message - INFO	This will inform you of events that do not require a response, such as a scan has started or stopped, or a completed scan found no viruses.

Lock Screen

This option locks InocuLAN's screen to prevent
unauthorized usage. When you lock the screen, you
give it a password. In order to unlock the screen, the
user must enter the same password that was used to lock
it.

To lock the screen:

1. Choose Lock Screen from the menu.

2. Enter a password.

    Be sure to remember the password you use.

3. Verify the password you entered.

    The screen remains locked until you unlock it.

To unlock the screen:

1. Press ENTER.

2. Enter the password.

How to Unload/Exit InocuLAN

This option unloads InocuLAN.

> NOTE: Unload GETBBS.NLM before unloading InocuLAN.

To unload InocuLAN:

1. Choose Exit from the menu.

2. Answer **Yes** to confirm.

Unloading from the
console

You may also unload InocuLAN from the server console screen. To do so, enter

SHUTDOWN INOCULAN

at the console. InocuLAN will unload. Note that this command will *not* work if the Lock Screen feature is active.

7

C h a p t e r

INOCULAN FOR DOS BASICS

This chapter describes the basic features of the InocuLAN for DOS Manager.

In this chapter, you will learn:

The InocuLAN for DOS Manager

To load InocuLAN for DOS on a workstation:

1. Change to the directory where the InocuLAN for DOS Manager is installed.

If you want to be able to manage the InocuLAN NLM, you must be connected to your network.

InocuLAN For DOS

2. Type InocuLAN to start InocuLAN for DOS.

If InocuLAN was installed using the Windows installation program, you can load InocuLAN by double-clicking the InocuLAN icon in the InocuLAN program group.

The InocuLAN program begins by checking the workstation's memory. If there are no viruses detected in RAM and INOCULAN.EXE is not infected, InocuLAN's Available Topics menu will be displayed.

If InocuLAN detects a virus loaded in memory, InocuLAN will neutralize the virus and display a message showing the number of viruses that were neutralized. Then, the Available Topics menu will appear.

> **NOTE:** Even though InocuLAN has removed the virus(es) from memory, you should reboot your workstation with a write-protected, clean boot diskette (such as the original operating system diskette) before continuing with InocuLAN for DOS. You should then refer to Chapter 8, "Scanning your Network with InocuLAN for DOS," for more information about removing the virus from your system.

InocuLAN network
functions

If you want to use InocuLAN's network functions, you must load InocuLAN on a server. See 'Loading InocuLAN' on page 6-2 for details.

Deactivating
InocuLAN

If you want to deactivate the InocuLAN NLM on the server, you can do so from within InocuLAN for DOS.

To deactivate InocuLAN:

1. Select *Domain Operation* from the Available Topics menu.

2. **Select the server on which you wish to deactivate InocuLAN and press ENTER.**

3. Select *Administration* from the Available Topics menu.

4. **Select *Deactivate InocuLAN NLM* from the Administration menu.**

   A message will ask you to confirm your choice. Select YES to deactivate InocuLAN.

   You may reactive InocuLAN by following the same procedure above, and selecting *Activate InocuLAN NLM* in Step 4.

Domain Security

InocuLAN protects your domains from unauthorized access by requesting a name and password the first time a domain is accessed.

After selecting the Domain Operation option, a window opens showing all available InocuLAN domains and single-servers. When you select a domain or server and press ENTER, a security window requests a name and password:

```
╔══════════════════════════════════════════════════════════════╗
║            Enter User ID and Password for NY-SUNNY            ║
╟──────────────────────────────────────────────────────────────╢
║ User Name: ▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓             ║
║  Password:                                                    ║
╚══════════════════════════════════════════════════════════════╝
```

After entering the correct information, you can perform all InocuLAN functions for as long as InocuLAN is running on your workstation. If you exit InocuLAN and restart it at a later time, you will again be asked for a password. Also, if you try to access a different domain or server, you will be asked for password information.

| NOTE: For NDS-only users: the Login ID you provide must be a distinguished (complete) name, for example: **ADMIN.ACCOUNTING.WORK** |
| --- |

The Basic InocuLAN for DOS Screens

There are three basic screens used in InocuLAN for DOS:

➢ Menus

➢ Lists

➢ Forms

Regardless of the type of screen, every screen has the same basic format.

The header contains basic information about your workstation and your version of InocuLAN for DOS. The footer lists all of the keys that are available on the current screen.

The following is an example of the InocuLAN for DOS main menu. The actual menu you see may be different, depending upon if you are a user or supervisor, if you are on a network, if you are on a network but are not logged in, or if you are on a stand-alone workstation.

This is the version of InocuLAN for DOS you are using.

This is the current date and time.

This is the address of your workstation.

```
Cheyenne InocuLAN <TM>  V4.0                    Monday  September 18, 1995  3:13 pm
                                                Local Address: 00000102-0000C08AED99
```

This section of the screen will vary depending upon where you are in InocuLAN for DOS.

```
                        Available Topics
                  Domain Operation
                  Run Scanner
                  Protect Critical Disk Area
                  View Scanning Records
                  Virus List
                  Version Information
                  DOS Shell
```

These are the keys that are available on this screen.

```
        <F1>:Help    <Enter>:Select    <Esc>:Exit
```

Menus   The InocuLAN for DOS Manager is menu-driven.

To select a menu option:

1. Use the arrow keys to highlight the desired option.

2. Press ENTER (or click the left mouse button).

Lists   A list is similar to a menu. It can be used to view information (as in the case of InocuLAN's Virus List), or, more commonly, to select one or more items from a group of options.

```
 ─                        InocuLAN for DOS                       ▼ ▲
Cheyenne InocuLAN <TM>  V4.0                 Thursday  August 31, 1995  8:05 am
                                             Local Address: 00000102-0000C0EB4796

 Execution Time   Source                        Action    Virus   Status
 09-06-95 02:44pm C:\AAAA                        Broadcast     0 Complete
 09-06-95 02:42pm C:\AAAA                        Broadcast     0 Complete




    <F1>:Help   <Del>:Delete   <Enter>:Select   <Ins>:Search   <Esc>:Exit
```

To select one item from a list:

1. Use the arrow keys to highlight the desired item.

2. Press ENTER (or click the left mouse button).

If a list allows you to select multiple items:

1. Use the arrow keys to highlight the desired item.

2. Press F5 to mark the item.

3. Repeat steps 1 and 2 until all of your items have been selected.

Forms   A form is used to enter data into fields.

Whenever possible, default values appear in the fields when a form is initially displayed.

Forms have three types of fields:

➢ Text Entry fields - allow you to enter information
➢ Toggle fields - allow you to select from two options
➢ List fields - allow you to select one or more items from a group of options

Details about entering information into each of these
types of fields appear on the next page.

Entering Information Into Fields

To enter information into any type of field, you must place the cursor in that field.

In order to place the cursor in a field:

1. Highlight the field.

2. Press ENTER (or click the left mouse button).

Text entry fields

Some text entry fields allow you to type in the information, such as a date or time.

Other text entry fields, such as those fields that require a valid server or workstation path, allow you to build the path by selecting from lists of servers, volumes, drives, and directories.

To access these lists from within one of these fields:

1. Press the INSERT key (or click the left mouse button).

2. Highlight an entry from the list.

3. Press ENTER (or click the left mouse button).
   The next level down in the directory tree will be displayed.

4. Repeat steps 2 and 3 until the desired path is displayed.
   You can select the ".." entry in the directory tree to remove the last entry you chose. This will return you to the previous level of the directory tree. (This is similar to the DOS command **CD..** which is used to return to one level higher in the directory tree.)

You can specify a particular file name by typing a backslash and then the file name.

5. Press ESC (or click the right mouse button).

Toggle fields   Toggle fields allow you to select from two options. To select an option:

1. Highlight the field and press ENTER.

2. Use the left/right arrow keys or a corresponding letter on your keyboard to select an option (or click the left mouse button).

List fields   List fields allow you to select one or more items from a group of options.

To select one item from a list:

1. Use the arrow keys (or mouse) to highlight the desired item.

2. Press ENTER (or click the left mouse button).

If a list allows you to select multiple items:

1. Use the arrow keys (or mouse) to highlight the desired item.

2. Press F5 to mark the item.

3. Repeat steps 1 and 2 until all of your items have been selected.

Keys Used in InocuLAN for DOS

The keys used by InocuLAN for DOS are described in the table below:

Key	Meaning	Function
F1	HELP	Accesses InocuLAN's online help. Press F1 a second time to display a list of keys that are used with InocuLAN for DOS.
F2	DONE	Executes a form and processes the information.
F3	MODIFY	Allows you to edit an item.
F5	MARK	Flags multiple items for selection.
F6	MARK ALL	Selects all items in a list. When viewing the Activity Log, this key captures the log in a file or sends it to a printer.
F7	SEARCH	Allows you to search a string. In a field, this key lets you cancel the changes you entered.
ENTER	SELECT	Selects a highlighted item, accepts the information you entered, and confirms selections.
ESC	ESCAPE	Returns you to the previous screen or exits you from InocuLAN for DOS.
INSERT	INSERT	Adds an additional item to a list or adds information to a field. When used with forms, this key displays path information.
DELETE	DELETE	Deletes an item from a list or deletes information from a field.
PAGE UP	PAGE UP	Returns to the previous page of a help screen, list, or file.

Key	Meaning	Function
PAGE DOWN	PAGE DOWN	Advances to the next page of a help screen, list, or file.
ARROWS	CURSOR CONTROL	Moves the cursor around a menu, list, form, or field. This key can also be used to toggle between options within a toggle field.
BACKSPACE	BACKSPACE	Deletes the character to the left of the cursor.
TAB	TAB	Moves the cursor around a form.

Using a Mouse With InocuLAN for DOS

InocuLAN for DOS allows you to use a mouse for many functions.

In order to use a mouse with InocuLAN, a mouse driver must be loaded on your workstation. Refer to the manual that came with your mouse for information about installing a mouse driver on your workstation.

If a mouse driver is loaded, the mouse pointer (a character block) will appear on your screen to the right of the Available Topics menu when InocuLAN for DOS is started.

Left mouse button

Use the left mouse button to select menu and list items. You can also move from field to field in a form and change the selection in a toggle field using the left mouse button.

Right mouse button

The right mouse button works like the ESCAPE key. It returns you to the previous screen or exits you from InocuLAN for DOS.

Online Help in InocuLAN for DOS

InocuLAN for DOS offers online help on every screen.

If you are on a menu or a list, the online help will display general information about that screen.

If you are on a form, the online help will display information about the specific field that you are in.

Accessing online help

To access online help from any InocuLAN for DOS menu, list, or form:

1. **Press F1.**

   Press F1 a second time to display a list of keys that are used with InocuLAN for DOS.

Version Information

You can display information about the version of InocuLAN for DOS installed on your domain server and on your workstation.

Displaying version information for your domain server

To display version information for your domain server:

1. **Select Domain Operation from the Available Topics menu.**

2. **Select a domain.**

   Highlight the domain you want and press ENTER.

3. **Select Version Information.**

   The following screen appears:

This screen contains version information for NetWare and InocuLAN on the selected domain server.

```
┌────────────────────────────────────────────────────────────┐
│                InocuLAN Version Information                 │
│                                                            │
│ Host Server Information                                    │
│                    Name : NY-SUNNY                         │
│            NetWare Version : NW V3.11                      │
│           InocuLAN Version : V4.00                         │
│      Signature File Version : V3.07                        │
│         Signature File Date : 08/09/95                     │
│             Engine Version : V3.05                         │
│                Engine Date : 09/11/95                      │
│                    Status : Active                         │
└────────────────────────────────────────────────────────────┘
```

Displaying version information for your workstation

To display version information for your workstation:

1. **Select Version Information from the Available Topics menu off of the main menu.**

   The following screen appears:

This screen contains version information for DOS, InocuLAN for DOS and signature files, as well as the location of system files.

```
┌──────────────────────────────────────────────────────────────┐
│                  InocuLAN Version Information                  │
├──────────────────────────────────────────────────────────────┤
│                                                                │
│ Workstation Information                                        │
│                 DOS Version : 5.00                             │
│              IO System File : C:\IO.SYS                        │
│             DOS System File : C:\MSDOS.SYS                     │
│                  Shell File : C:\COMMAND.COM                   │
│        INOCULAN.EXE Version : 4.0                              │
│ Local Signature File Version : 03.06 08/22/1995               │
│                                                                │
│                 Press Any Key To Continue                      │
│                                                                │
└──────────────────────────────────────────────────────────────┘
```
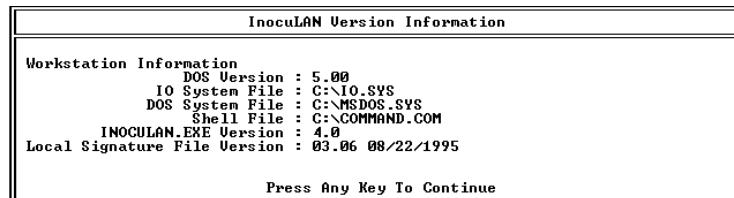
Exiting to DOS

While you are using InocuLAN for DOS you can temporarily exit and go to DOS to execute DOS commands.

While InocuLAN for DOS is loaded and a scan is running on a workstation, IMMUNE is disabled. This eliminates double scanning operations.

Instructions for exiting to DOS

To temporarily exit to DOS:

1. Select DOS Shell from the Available Topics menu.

You will be brought to the DOS prompt.

2. Type Exit when you are ready to return to InocuLAN for DOS.

If the path to your COMMAND.COM file is incorrect (for example, your user login script set the path, but your server connection has been lost) you may need to use the DOS command SET COMSPEC to help InocuLAN for DOS locate your COMMAND.COM.

The following examples illustrate how you might use the SET COMSPEC command:

SET COMSPEC=D:\COMMAND.COM

SET COMSPEC=C:\COMMAND.COM

SET COMSPEC=C:\BIN\COMMAND.COM

Viewing the Activity Log

The Activity Log contains information about the operations performed by InocuLAN for DOS. The log tells you when:

> ➣ InocuLAN is loaded on your server.
> ➣ A virus is discovered by IMMUNE or the Real-time Monitor. (Viruses detected by the Run Scanner or Schedule Server Scanner are reported in the Scanning Reports.)
> ➣ The server's virus signature file is updated.

Although each InocuLAN domain server has its own Activity Log, the master server's Activity Log will report information about viruses discovered by IMMUNE or the Real-time Monitor on member servers. For more information about domains, refer to Chapter 9.

NOTE: This is the same Activity Log that you can view from the InocuLAN Server menu.

Instructions for displaying the Activity Log

To display the Activity Log:

1. Select Domain Operation from the Available Topics menu.

2. Select a domain.

   Highlight the domain you want and press ENTER.

3. Select View Activity Log.

   A screen similar to the one shown below appears:

Information in the log appears in chronological order. Press the END key twice to move to the end of the log.

```
INFO 11/17/95 07:27AM InocuLAN Server is Ready
WARN 11/17/95 07:27AM Enforcement Activated by Console
WARN 11/17/95 07:27AM Enforcement Deactivated by Console
CRIT 11/17/95 03:39PM Real-time Configuration: Checking: Incoming/Outgoing Fil
CRIT 11/17/95 03:59PM Real-time Configuration: Checking: Incoming/Outgoing Fil
INFO 11/17/95 04:07PM Start IMMEDIATE SCAN JOB #0.
INFO 11/17/95 04:12PM End SCAN JOB #0.
CRIT 11/18/95 07:00AM Real-time Configuration: Checking: Incoming/Outgoing Fil
INFO 11/18/95 07:00AM InocuLAN Server is Ready
INFO 11/18/95 07:06AM Start IMMEDIATE SCAN JOB #1.
INFO 11/18/95 07:06AM End SCAN JOB #1.
INFO 11/18/95 07:06AM Start IMMEDIATE SCAN JOB #1.
INFO 11/18/95 07:06AM End SCAN JOB #1.
WARN 11/18/95 07:10AM InocuLAN Server is Deactivated By Console
INFO 11/18/95 07:10AM InocuLAN Server is Ready
WARN 11/18/95 07:10AM Enforcement Activated by Console
WARN 11/18/95 07:10AM Enforcement Deactivated by Console
INFO 11/18/95 07:10AM Updating Virus Signature, InocuLAN Was Deactivated Tempo
```

Searching the Activity Log

You can search the Activity Log for any text. For example, you might want to find out which files were affected by a specific virus. To do this, you would search the Activity Log for the virus name. You could then repeat the search to find the next occurrence of the virus.

To search for text:

1. Press F7 to bring up the search window.

2. Enter the string of text you want to find.

You can enter any text, including a date, time, virus name or file name (for example: 05/19/94 or MICHELANGELO).

3. Press ENTER.

You will be brought to the first occurrence of the text string you entered.

4. Press SHIFT and F7 together to search for the same text string again.

Printing the Activity Log

You can create a report from the Activity Log. This report can be sent directly to a printer or it can be captured in a file and printed at a later time.

To print the Activity Log:

1. Press F6.

2. Enter a path and file name for the report.

    To print to a printer, enter the printer port, such as
    LPT1.

    If you are capturing the log to a file, you can press
    the INSERT key to help specify the path.

    The report file that is created will be in ASCII
    format.

**Configuring the
Activity Log**

You can choose what kinds of messages the log will
record and the number of messages it will store.

To configure the Activity Log:

1. Select Domain Operatiorfrom the Available Topics menu.

2. Select a domain.

    Highlight the domain you want and press ENTER.

3. Select Administration

4. Select Activity Log Configuration

    The Activity Log Configuration screen appears:

```
┌─────────────────────────────────────────────────┐
│          Activity Log Configuration             │
├─────────────────────────────────────────────────┤
│  Maximum Entries:                          200   │
│  Purge After n Number of Days:             30    │
│  Include Critical Events:                  YES   │
│  Include Warnings:                         YES   │
│  Include Informational Messages:           YES   │
└─────────────────────────────────────────────────┘
```

5. Select the Activity Log Configuration options.

Maximum Entries	The maximum number of messages that should remain in the Activity Log. Values range from 10 to 1000 messages.
Purge After n Number of Days	Indicates how long, in days, you want to keep an event in the log. Values range from 1 to 365 days.
Include Critical Events	Indicates whether Critical messages should be logged. Critical messages are the highest level messages. They require immediate attention once logged. This message could mean there is a virus detected, or there is a serious problem with the network. This is the default value and cannot be changed.
Include Warnings	Indicates whether Warning messages should be logged. Warning messages are second priority, informing you that InocuLAN has skipped a file or other non-critical information. Select yes or No.
Include Informational Messages	Indicates whether Informational messages should be logged. Informational messages include messages that InocuLAN has stopped or started, and that no viruses have been found. Select Yes or No.

Virus List

You can display a list of the viruses that InocuLAN for DOS can detect. You can also print this list.

To display the list:

1. Select Virus List from the Available Topics menu.

The list is displayed:

This is a section of the list of viruses that InocuLAN for DOS can detect.
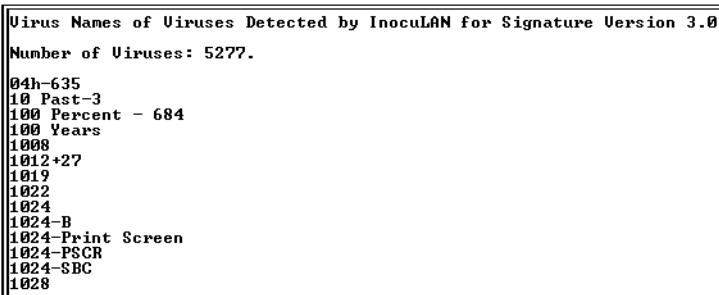
```
Virus Names of Viruses Detected by InocuLAN for Signature Version 3.0

Number of Viruses: 5277.

04h-635
10 Past-3
100 Percent - 684
100 Years
1008
1012+27
1019
1022
1024
1024-B
1024-Print Screen
1024-PSCR
1024-SBC
1028
```

Searching for a specific virus

You can search the virus list for a specific virus name. To search:

1. Press F7 to bring up the search window.

2. Enter the virus name you want to find.

3. Press ENTER.

If you want to search for the same text again, press SHIFT and F7 together.

Printing the virus list

You can create a report from this list. This report can be sent directly to a printer or it can be captured in a file and printed at a later time.

To create a report:

1. Press F6.

2. Enter a path and file name for the report.

   Enter the printer port (LPT1, for example) to send the report to the printer.

   To capture the report to a file, you can press INSERT to display available servers, drives, and directories.

8

C h a p t e r

SCANNING YOUR NETWORK WITH INOCULAN FOR DOS

InocuLAN for DOS helps keep your network virus-free.

In this chapter, you will learn:

Scanning Basics

There are two scanners you can use to scan your network from the InocuLAN Manager:

> ➣ Schedule Server Scanner
> ➣ Run Scanner

You can also initiate a scan of a domain server directly from the server console. Refer to Chapter 8, "Server Commands", for more information.

If you want to scan a Macintosh workstation, you can use InocuLAN for Macintosh. Refer to Chapter 10, "Installing and Using InocuLAN for Macintosh" for more information.

Schedule Server Scanner

The Schedule Server Scanner lets you administer scanning jobs on all of your domain servers. You can run the scan immediately or schedule it to start at a later time. Scanning can be repeated at regular intervals. This function is only available for supervisors or supervisor equivalents.

Run Scanner

The Run Scanner scans files on a local workstation or a mapped drive. The server does not have to be an InocuLAN domain server.

Selecting the correct scanner

If you cannot decide which scanner you need to use, refer to the following table. This table summarizes the basic functions of each scanner:

	What is scanned	File types	Who can use this scanner	Scanning occurs
Submitted by Schedule Server Scanner	InocuLAN domain server volumes	DOS, Windows and Mac	Supervisor or equivalent	Immediate, scheduled, or repeated at periodic intervals
Executed by Run Scanner	Any server*, local workstation, or floppy diskette	DOS and Windows	User or Supervisor	Immediate

* You cannot use the Run Scanner for a server that has real-time scanning enabled. Viruses will be reported by the Real-time Monitor.

Using the Schedule Server Scanner

The Schedule Server Scanning option scans files on a domain server. The scanning can be scheduled or it can be run immediately. Scanning can be repeated at varying intervals. The actual scanning is done by InocuLAN's NLM on the server.

If you are using domains, you can scan all of your domain members by setting up one scan job. The information for the scanning job will be propagated to all of your domain members. Therefore, by setting up a job to scan the SYS volume on your master server, you will scan the SYS volume on all of your domain member servers. You may also enter an asterisk (*) to scan all volumes.

Instructions for using the Schedule Server Scanner

Follow the instructions below for using the Schedule Server Scanner:

1. **Select Domain Operation from the Available Topics menu.**

2. **Select a domain.**

   Highlight the domain you want and press ENTER.

3. **Select Administration**

4. **Select Schedule Server Scanning**

   The Scheduled Job List screen is displayed:

This screen will be
blank initially.

```
Owner         Execution Time   Source                      Action       Status
Console Oper 09/18/95 09:39AM SYS:\NORTON               Report Only    DONE
Console Oper 09/18/95 09:45AM SYS:\ACCESS               Report Only    DONE
Console Oper 09/18/95 09:46AM SYS:                      Report Only    DONE
Console Oper 09/18/95 10:40AM SYS:\HPSERVER             Report Only    DONE
Console Oper 09/18/95 10:41AM SYS:\ACCESS               Report Only    DONE
Console Oper 09/18/95 11:52AM SYS:\ACCESS               Report Only    DONE
             09/18/95 01:21PM SYS:                      Report Only    READY
Local        09/18/95 02:20PM *                         Report Only    READY
```

This screen displays a summary of all scheduled
jobs in the queue. The *Status* field will say ACTIVE
if the job is currently being processed. It will say
READY if the job is waiting in the queue to be
processed.

If you want to change a scheduled job, highlight the
job and press ENTER.

If you want to delete a scheduled job, highlight the
job and press DELETE.

5. Press INSERT to create a new job.

    If you press INSERT, the Schedule Server Scanning
    form will be displayed:

```
                    Schedule Server Scanning Form
Source Directory:       SYS:
Traverse Directory:     YES
File Selection:         <Press Insert Key For List>
Scan Type:              Secure
Scan Compressed Files?  YES    File Extensions:<Press Insert Key For List>
Skip NetWare Compressed:YES
Start Scan          on:11/22/95   at:2:55 pm
Repeat Interval:        0  Months    0 Days    0 Hours    0 Minutes
Repeat Scan Days:       Sun:YES Mon:YES Tue:YES Wed:YES Thu:YES Fri:YES Sat:YES
Action Upon Virus Detection:   Report Only
Print Report:                  On Virus Only
    Printer Server:            NY-WRITER
    Queue:                     HLPJ4
    User Name:                 PETER
    Password:                  ******
Delay If CPU Utilization Up To 99 %
```

Printer
information
appears only if
a print option
has been
selected.

6. Enter information on the Schedule Server Scanning form.

Source Directory	If this is a multi-server domain, enter the volume to scan. An asterisk (*) indicates that all volumes will be scanned.
	If this is a single server domain, you can select a specific directory to scan.
	Press the INSERT key twice to display available volumes and directories.
Traverse Directory	Select Yes to scan all subdirectories under the source directory or No to scan only the source directory. For example, if you answer No and an entire server volume is selected as the source directory, only its root will be scanned.
File Selection	Press INSERT twice to select specific types of DOS and Macintosh files for scanning.
	For *DOS files*, you can select all files or a selection of executable files. If you select *EXECUTABLE FILES*, you can further define which files to scan by their extensions.
	For *Macintosh files*, you can select all files, application type files, or files with a resource fork (the portion of a Macintosh file that contains the program code, font information, and other data not normally generated by a user). You can also choose not to scan Macintosh files.
	If you select *ALL FILES* for your DOS scan selection, the Files Excluded List will be displayed:
	You can exclude specific files or directories from being scanned. For example, you might want to exclude all files in a directory used for research purposes only.
	To specify a file or directory, press ENTER. If this is a single server domain, you can press the INSERT key twice to choose from available volumes and

```
╔══════════════════════════════════════════════════════╗
║                    Files Excluded                    ║
╟──────────────────────────────────────────────────────╢
║ Exclude Files List                                   ║
║     WRITER/SYS:\ELLEN\*.*                            ║
║     WRITER/SYS:\*.BAK                                ║
║     WRITER/SYS:\ARCSERVE\ARCSERVE.HLP               ║
║                                                      ║
║                                                      ║
║                                                      ║
║                                                      ║
║                                                      ║
║                                                      ║
║                                                      ║
║                                                      ║
║  <F1>:Help <F2>:Done <Enter>:Modify <Ins>:Insert <Del>:Delete ║
╚══════════════════════════════════════════════════════╝
```
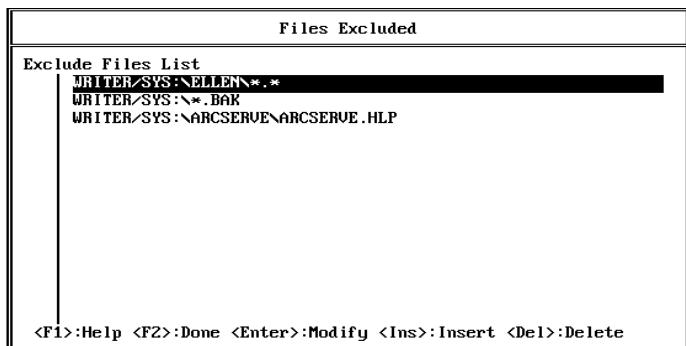
directories. If this is a multi-server domain, type in the file name or directory to exclude.

You can use wildcards. For example, you could use a wildcard to exclude files with a specific extension (such as *.BAK).

If you want to specify an entire directory, type *.* after the directory name (for example: WRITER/SYS:\MANUAL*.*).

Since a file or directory may not exist on every server volume, InocuLAN will only apply the exclusion to those server volumes that contain the file or directory you specified.

Select Yes if you want InocuLAN to check just the beginning and end of each data file. Select No if you want InocuLAN to examine the whole file. This is a thorough way to check files but is slower than running a fast scan.

This option only applies to data files. Other types of files (*.EXE, *.COM, etc.) are always fully scanned.

Scan Type　　　　　Select one of the following Scan Types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Scan Compressed Files	Select this option for InocuLAN to scan compressed files. By default, InocuLAN scans files of the ZIP and ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, press Insert in the *File Extensions* field.
Skip Netware Compressed	This option will cause InocuLAN to avoid scanning any NetWare compressed files on your servers. This is the default value. Scanning compressed files will increase the scanning time.
Start Scan	A scan can be run immediately or it can be scheduled for a later date or time. The default is the current date and time.
Repeat Interval	If you want the scan to take place a single time, these fields should be set to zero. If the file server scanning is to be repeated automatically, enter the time interval between each scan.
Repeat Scan Days	If you don't want scanning to take place on particular days, such as over the weekend, you can turn off scanning with these fields. By default, all days are set to YES. To change a day to NO, highlight the field and enter "N".

Action Upon Virus Detection

Press ENTER to display a list of options. Regardless of which option you choose, a message will be broadcast when a virus is detected.

Action	Description
Broadcast	Sends messages via Broadcast, MHS, FAX, SNMP, Trouble Ticket, and Pager, if they have been set up. The message also appears in the Scanning report.
Delete File	Deletes an infected file from the server.
Rename File	Renames infected files by giving them an AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners (except the Real-time Monitor). (See the note on the next page for Macintosh files.) If a file exists with the AVB extension and an infected file in the same directory will result in the same file name, the AVB extension will be changed. The extension will become AV# and the number will be incremented for each subsequent occurrence (AV0, AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to 'Rename File' above). Even if InocuLAN cures the file, we recommend you purge the infected file and then restore the original file.
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory. (See the note on the next page for Macintosh files.)
Purge File	Deletes an infected file so that it cannot be recovered (for example, using Novell's Salvage utility).

Action	Description
Move and Rename File	Renames infected files by giving them a different extension and then moves them to the INOCULAN\VIRUS directory. (See the note below for Macintosh files.)

NOTE: If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

NOTE: An infected Macintosh file cannot be renamed or moved.

Every Macintosh file has a file type. If a virus is found, the file type is changed to prevent the file from being used and prevent the virus from spreading. The file types are:

Macintosh File Type	New File Type
Application - APPL	INOA
Data - DATA	INOD
Resources - RSRC	INOR
Stack - STAK	INOS
Text - TEXT	INOT

Print Report

There are three printing options available after a scan. To select an option, highlight the field and press ENTER, then choose one of the options:

Print Report option	Description
No Printing	No report will be printed following the scan.

Print Report option	Description
Print Always	A report will be generated following every scan.
On Virus Only	A report will be generated only if a virus is detected.

If you select the Print Always or On Virus Only options, additional fields will appear on the Schedule Scanner Scanning form.

Field	Description
Printer Server	Enter the name of the server you are using. To choose from a list of available servers, highlight the field and press INSERT.
Queue	Enter the NetWare printer queue name. If you do not know your printer queue name, type PCONSOLE at the DOS command line and press Enter to access the NetWare Print Console. Select Queue Information from the menu to see your print queue choices. Press ESC to exit the Print Console. If you need additional instructions on how to use the Print Console, consult your network administrator. For an NDS queue, you must provide a distinguished (complete) name.
User Name	Enter the server user name.
Password	Enter the server password.

Delay If CPU Utilization Up To %

Enter a CPU Utilization percentage to indicate the point at which InocuLAN scanning should slow down. (CPU Utilization represents the percentage of time the file server CPU is being used.)

7. **Press F2 when the form is complete.**

8. **Answer Yes to confirm.**

Checking the Results of Your Scan

Follow the instructions below to see the results of the Schedule Server Scan:

1. Select *Domain Operation* from the Available Topics menu.

2. Select a domain.

    Highlight the domain you want and press ENTER.

3. Select *View Scanning Records.*

```
 Execution Time     Source                          Action     Virus  Status
↑09-18-95 12:45pm NY-SUNNY\SYS:\ACCESS           Report Only     0 Complete
 09-17-95 07:20am NY-SUNNY\*                      Report Only     0 Complete
 09-18-95 01:41pm NY-SUNNY\SYS:\ACCESS           Report Only     0 Complete
 09-18-95 02:52pm NY-SUNNY\SYS:\ACCESS           Report Only     0 Complete
 09-18-95 09:26am NY-SUNNY\SYS:                  Report Only     0 Complete
 09-16-95 03:20pm NY-SUNNY\*                      Report Only     0 Complete
 09-18-95 01:20pm NY-SUNNY\*                      Report Only     0 Complete
 09-16-95 03:20am NY-SUNNY\*                      Report Only     0 Complete
 09-18-95 02:21pm NY-SUNNY\SYS:                  Report Only     0 Complete
 09-16-95 07:26am NY-SUNNY\SYS:                  Report Only     0 Complete
 09-16-95 06:21am NY-SUNNY\SYS:                  Report Only     0 Complete
 09-18-95 10:21am NY-SUNNY\SYS:                  Report Only     0 Complete
 09-18-95 12:21pm NY-SUNNY\SYS:                  Report Only     0 Complete
 09-18-95 03:27pm NY-SUNNY\SYS:                  Report Only     0 Complete
 09-18-95 12:39pm NY-SUNNY\SYS:\NORTON           Report Only     0 Complete
↓09-18-95 03:26pm NY-SUNNY\*                      Report Only     0 Canceled
```

This screen displays the results of all Schedule Server Scanning jobs (including jobs run on domain member servers).

Scans run with the Run Scanner are not displayed on this screen. Refer to the 'Using the Run Scanner' section, which begins on page on page 8-16, for more information.

4. Highlight the job you want to find out more information about.

5. Press ENTER.

This screen displays detailed information about the scanning job. You can print this information or search for specific text.

```
                    ServerName : NY-SUNNY
09/16/95 21:20 Start SCHEDULED SCAN.     Volume - SYS:
09/16/95 21:20 All Dos Files Will be Checked
09/16/95 21:20 All Mac Files Will Be Checked
09/16/95 21:20 Infected Files Will be Recorded
09/16/95 21:20 Delay If CPU Utilization Up to: 25    Scan Type: Fast
09/16/95 21:20 Traverse Directory: Yes
               128,069 KBytes   in 1,257 Files in 85 Directories Have Been Scan
               No Viruses Detected
               Total Elapsed Time : 00:06:26
```

Configuring the Scan Log

You can choose what kinds of messages the log will record and the number of messages it will store.

To configure the Scan Log:

1.   Select Domain Operation from the Available Topics menu.

2.   Select a domain.

Highlight the domain you want and press ENTER.

3.   Select Administration

4.   Select Scan Log Configuration

The Scan Log Configuration screen appears:

```
┌───────────────────────────────────────────┐
│         Scan Log Configuration            │
├───────────────────────────────────────────┤
│  Maximum Entries:                    100  │
│  Purge After n Number of Days:       30   │
│  Include Critical Events:            YES   │
│  Include Warnings:                   YES   │
│  Include Informational Messages:     YES   │
└───────────────────────────────────────────┘
```

5.   Select the Scan Log Configuration options.

| Maximum Entries | The maximum number of messages that should remain in the Activity Log. Values range from 1 to 1000 messages. |

| Purge After n Number of Days | Indicates how long, in days, you want to keep an event in the log. Values range from 1 to 365 days. |

| Include Critical Events | Indicates whether Critical messages should be logged. Critical messages are the highest level messages. They require immediate attention once logged. This message could mean there is a virus detected, or there is a problem with the service. This is the default setting and it cannot be changed. |

| Include Warnings | Indicates whether Warning messages should be logged. Warning messages are second priority, informing you that InocuLAN has skipped a file or other non-critical information. Select yes or No. |

| Include Informational Messages | Indicates whether Informational messages should be logged. Informational messages include messages that InocuLAN has stopped or started, and that no viruses have been found. Select Yes or No. |

Using the Run Scanner

The Run Scanner scans files on a local workstation or a server. The server does not have to be an InocuLAN domain server, but you must be connected to the server. The actual scanning is done by INOCULAN.EXE on the local workstation.

NOTE: You cannot use the Run Scanner for a server that has real-time scanning enabled. Viruses will be reported by the Real-time Monitor. Instead of the Run Scanner, you can use the Schedule Server Scanner for these servers.

Instructions for using the Run Scanner

Follow the instructions below for using the Run Scanner:

1. Select Run Scanner from the Available Topics menu on the main menu.

   The Scanner Form will be displayed:

   ```
   ┌──────────────────────────────────────────────────────────────┐
   │                         Scanner Form                          │
   ├──────────────────────────────────────────────────────────────┤
   │  Source Directory: C:\                                        │
   │  Traverse Directory: YES                                      │
   │                                                              │
   │  Report File: VIRUS.TXT                                      │
   │  Append Report File: YES                                     │
   │                                                              │
   │  File Selection: <Press Insert Key For List>   Scan Type: Secure │
   │  Scan Compressed Files?  YES                                 │
   │  Compressed File Extensions:<Press Insert Key For List>      │
   │                                                              │
   │  Action Upon Virus Detection: Report Only                   │
   │                                                              │
   └──────────────────────────────────────────────────────────────┘
   ```

2. Enter information on the Scanner Form.

Source Directory

Enter the directory where scanning should start. You can select the entire server, a server volume, or a specific directory. An asterisk indicates that all local hard drives will be scanned.

Press INSERT twice to display available drives, servers, volumes, directories, and subdirectories. Press ESC after you have made your selections.

Traverse Directory

Enter Yes to scan all subdirectories under the source directory or No to scan just the source directory. For example, if you answer No and an entire server volume is selected as the source directory, only its root will be scanned.

Enter Yes for InocuLAN to scan compressed files in your directories. To skip compressed files, enter No.

Report File

Enter a path and file name for a report of the scan. You can press the INSERT key to help select the path.

The report will show the number of files and directories scanned, the number of infected files found, and the action taken. If an infected file is found, the virus responsible will also be listed. Press ESC when done.

Append Report File

Indicate if you want the report to append to the report file you named in the previous field. If you answer No, an existing report file will be overwritten.

Skip CD-ROM

Selecting this option will cause InocuLAN to *not* scan CD-ROM drives on your workstation. Note that this field only appears if you have a CD-ROM drive on your machine.

File Selection

Press INSERT twice to select specific types of DOS files for scanning.

You can select all files or a selection of executable files. If you select *EXECUTABLE FILES*, you can

further define which files to scan by their
extensions.

If you select *ALL FILE*S, the Files Excluded list will be displayed:
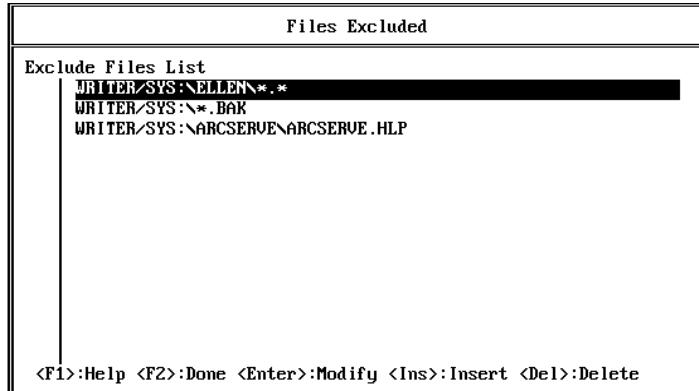
```
┌────────────────────────────────────────────────────────────┐
│                      Files Excluded                        │
├────────────────────────────────────────────────────────────┤
│ Exclude Files List                                         │
│     WRITER/SYS:\ELLEN\*.*                                  │
│     WRITER/SYS:\*.BAK                                      │
│     WRITER/SYS:\ARCSERVE\ARCSERVE.HLP                      │
│                                                            │
│                                                            │
│                                                            │
│                                                            │
│                                                            │
│                                                            │
│                                                            │
│                                                            │
│  <F1>:Help <F2>:Done <Enter>:Modify <Ins>:Insert <Del>:Delete │
└────────────────────────────────────────────────────────────┘
```

You can exclude specific files or directories from being scanned. For example, you might want to exclude all files in a directory used for research purposes only.

To specify a file or directory, press ENTER. You can then press INSERT to choose from available servers, drives, volumes, directories, and subdirectories.

You can use wildcards. For example, you could use a wildcard to exclude files with a specific extension (such as *.BAK).

If you want to specify an entire directory, type *.* after the directory name. For example:

WRITER/SYS:\MANUAL*.*

Scan Type	
Select one of the following Scan Types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only* option is selected.

Scan Compressed Files

Select this option for InocuLAN to scan compressed files. By default, InocuLAN scans files of the ZIP and ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, press Insert in the *Compressed File Extensions* field.

Action Upon Virus Detection

Press ENTER to display a list of options. Regardless of which option you choose, a message will be broadcast when a virus is detected.

Action	Description
Report Only	Displays an on-screen report that lists the infected files and the virus that was detected. This information also appears in the Scanning report.
Delete File	Deletes an infected file from the server.
Rename File	Renames infected files by giving them an AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners (except the Real-time Monitor). If a file exists with the AVB extension and an infected file in the same directory will result in the same file name, the AVB extension will be changed. The extension will become AV# and the number will be incremented for each subsequent occurrence (AV0, AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (see *Rename File* above). Even if InocuLAN cures the file, we recommend you purge the infected file and then restore the original file.
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory.
Purge File	Deletes an infected file so that it cannot be recovered (for example, using Novell's Salvage utility or DOS's Undelete).

Action	Description
Move and Rename File	Renames infected files by giving them a different extension and then moves them to the INOCULAN\VIRUS directory.

NOTE: If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

3. Press F2 when the form is complete.

4. Answer **Yes** to confirm.

   The scanner activity will be displayed on your screen.

Checking the Results of Your Scan

Follow the instructions below to see the results of the Run Scanner job:

1. Select View Scanning Records from the Available Topics menu.

```
Execution Time    Source                              Action      Virus   Status
5-9-94   3:54pm  NY-WRITER/VOL1:\ARCSOLO.OS2\GRA Broadcast        0 Complete
5-9-94   3:53pm  C:\ELLEN                            Broadcast        0 Complete
4-28-94  3:38pm  NY-DENEVAN/VOL1:\ALERT              Broadcast        0 Complete
3-29-94  11:46am C:\ARCSOLO                          Broadcast        0 Complete
```

This screen displays the results of scans run with the Run Scanner.

Scans run with the Schedule Server Scanner are not displayed on this screen. Refer to the previous section, 'Using the Schedule Server Scanner' for more information.

2. Highlight the job you want to find out more information about.

3. Press ENTER.

This screen displays detailed information about the scanning job. You can print this information or search for

```
Cheyenne InocuLAN for Windows

Report For Scan Executed On  11/29/95  At 10:11 AM

Drive Scanned                 : A


Total Boot Virus Infections   : 1
Total Boot Infections Cured   : 1

Total Directories Scanned     : 1
Total Files Scanned           : 13
Total Viruses Found           : 3

Total Files Infected          : 2
Total Files Cured             : 2
Total Files Deleted           : 0
Total Files Purged            : 0
```

9

GUARDING YOUR NETWORK

An integral part of the process of keeping your network virus-free is preventing viruses from gaining access to your network.

In this chapter, you will learn:

Keeping Your Network Virus-free

While you can use InocuLAN for DOS *just* to detect and cure problems caused by viruses, the best way to keep your network virus-free is to prevent viruses from gaining access to your network in the first place.

InocuLAN for DOS features

InocuLAN for DOS offers many features that, when used together, provide a solid barrier against viruses. These features are discussed briefly below. Detailed information about each feature can be found in this chapter.
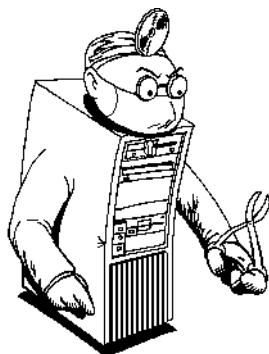
> **DOMAINS** allow you to group your InocuLAN servers so that they can share configuration information and resources. This helps you maintain your virus-free network with minimal effort.

> **REAL-TIME MONITOR** continually scans files on a domain server and workstations. Files can be scanned on an incoming or outgoing basis, or both.

> **IMMUNE** is a TSR that scans files on a workstation for viruses each time a file is executed, accessed, or opened. It can also be set to monitor the workstation for virus-like behavior, such as unauthorized formatting of the hard disk. IMMUNE can be used on all workstations, even workstations that do not have an InocuLAN Manager installed.

> **EXAMINE** is a program that checks a workstation for boot viruses. The workstation's Critical Disk Area is examined for changes, including infection and corruption.

➢ **ENFORCEMENT** prevents viruses from being copied to an InocuLAN/ NLM file server by forcing users to have IMMUNE loaded before they can log into the server.

➢ **CRITICAL DISK AREA PROTECTION** safeguards a workstation's hard disk. The Critical Disk Area includes the boot sector, partition table, CMOS RAM information, and DOS system files.

➢ **AUTOMATIC CHEYENNE BBS DOWNLOAD AND AUTOMATIC SERVER UPDATES** keep all of your InocuLAN servers synchronized with the most current virus signature files.

The InocuLAN for DOS scanners

In addition, InocuLAN for DOS has two scanning options that you can use to scan your network. They are discussed briefly below. Detailed information about these scanners can be found in Chapter 8, "Scanning your Network with InocuLAN for DOS."

➢ **Schedule Server Scanning** lets you administer scanning jobs on all of your domain servers. You can run the scan immediately or schedule it to start at a later time. Scanning can be repeated at regular intervals. This function is only available for supervisors or supervisor equivalents.

➢ **Run Scanner** scans files on a local workstation or on a mapped drive. The server does not have to be an InocuLAN domain server.

General suggestions

In addition to all of the InocuLAN for DOS features, we offer the following general suggestions to help keep your network virus-free:

➢ Set all of your executable files as Read Only files. Since a virus has the access rights of the user, making these files Read Only will reduce the chance of executable files becoming infected with viruses by non-supervisor users.

You can also use the more restrictive Execute Only option for executable files. *Make sure you are aware of the restrictions that may apply to these files.* For example, when you set a file to Execute Only, you may not be able to remove this setting, or back up the file. Refer to your *Novell Utilities Reference Manual* for more information about setting rights before you proceed.

➢ Be careful with supervisor privileges. Logging in as a supervisor or having supervisor-equivalent privileges gives you access to the file server's directory structure. This means you can infect the entire directory structure if your workstation is infected with a virus. Therefore, you should not log in as a supervisor unless you actually need supervisory privileges to perform a task.

➢ Do not grant users read, open, or search rights to other users' directories. Viruses can be spread if a user executes an infected program or copies an infected file from another directory.

➣ Cold-boot your workstation from a virus-free boot diskette before running InocuLAN for DOS.

➣ Use InocuLAN for DOS to scan floppy diskettes for viruses before copying any files from them.

➣ Back up your network after you successfully scan the network for viruses. This way, if InocuLAN for DOS detects a file with a virus that cannot be cured, you can restore a backed up version of that file.

Domains

A domain is a group of one or more InocuLAN servers (servers with the InocuLAN Server installed) that can share configuration information and resources.

Each domain contains one *master server*. All other servers in a domain are considered *member servers*.

What are the benefits of a domain?

A domain can be managed as a single entity. This has several benefits:

➢ You only have to enter configuration information once because all domain information is stored in the master server. The configuration information you enter for your master server automatically configures all of your member servers at the same time. (If necessary, each member server can have its own configuration.)

➢ Using the InocuLAN for DOS Schedule Server Scanner, you can scan all of your domain members by setting up one scan.

➢ All of the scanning reports on member servers are collected by the master server. Therefore, from your master server, you can see all of the activities of your member servers.

What type of information is shared by domain members?

The following is shared by all members of a domain:

➢ Real-time Monitor configuration
➢ Schedule Server Scanning configuration

- ➢ Activation/Deactivation of InocuLAN NLM
- ➢ Enforcement list

Creating a Domain

In order to enjoy the benefits of a domain, you must create a domain.

⚠️

> NOTE: Before you can create a domain, you must install
>   InocuLAN on each server that will be in your domain.

Do the following to create a domain:

1. Select Domain Operation from the Available Topics menu.

    A window appears showing the available servers.

```
 Domain Name    Master Server Name

                         SERVER1
                         SERVER2
                       NY-NW40-ALEX
                      ▼NY-PETER312
 DOMAIN-1             NY-SUNNY
 VICTOR3              NY-VICTOR311
                       └ BORG-11
 PAUL-DOMAIN          NY-K
                       ├ NASH
                       ├ NY-GIANTS
                       └ NY41
 MIGUEL               NY-LOCUTUS
 VICTOR               NY-WORF
```

These servers
are available
to include in a
domain.

This is an
existing multi-
server domain.

An inverted triangle indicates that
InocuLAN is not active on the server.

2. Press INSERT.

    The Domain Form appears:

Enter a name for your domain.

Indicate which server should be
the master. You can press
INSERT to select a server.

```
                            Domain Form

               Domain Name: BLDG1
        Master Server Name: NY-SUNNY
```

3. Enter a name for the Domain in the Domain Name field.

Designating the
master server

**4. Select a server in the Master Server Name field and press
ENTER.**

To choose from a list of available servers, press
INSERT twice.

5. Press F2 to create the domain.

You will need to log in to the server.

Adding Member Servers

You can add additional servers to your domain using the following procedure:

1. Highlight the newly created domain.

2. Press ENTER.

3. Select Member Servers.

    A list of all existing members (if any) will be displayed.

4. Press INSERT.

5. Select a server from the Domain Members list.

    You will need to log in to this server.

Checking the Status of domain members

To see the status of a server in an existing multi-server domain:

1. Highlight a server and press enter.

2. Select Server Status from the Available Topics menu.

    The Server Status window appears containing information on the selected server.
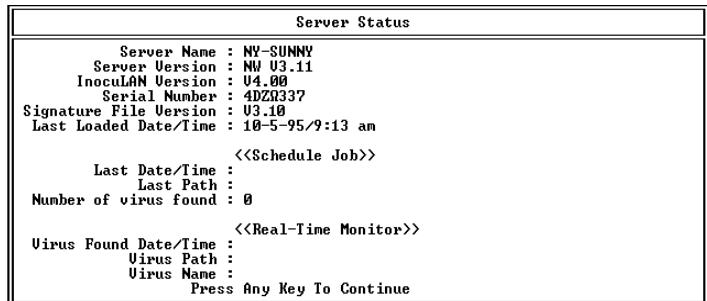
```
┌─────────────────────────────────────────────────────────────┐
│                        Server Status                         │
├─────────────────────────────────────────────────────────────┤
│              Server Name : NY-SUNNY                           │
│           Server Version : NW V3.11                          │
│         InocuLAN Version : V4.00                             │
│           Serial Number : 4DZΩ337                           │
│   Signature File Version : V3.10                            │
│     Last Loaded Date/Time : 10-5-95/9:13 am                 │
│                                                              │
│                      <<Schedule Job>>                        │
│           Last Date/Time :                                   │
│                Last Path :                                   │
│      Number of virus found : 0                              │
│                                                              │
│                    <<Real-Time Monitor>>                     │
│      Virus Found Date/Time :                                 │
│               Virus Path :                                   │
│               Virus Name :                                   │
│                 Press Any Key To Continue                    │
└─────────────────────────────────────────────────────────────┘
```

Real-time Monitoring on the Server

The Real-time Monitor scans files on a domain server in real-time. Files can be scanned on an incoming or outgoing basis, or both.

Your Real-time Monitor configuration will be shared by all members of the domain.

Instructions for configuring the Real-time Monitor

Follow the instructions below for configuring the Real-time Monitor:

1. **Select Domain Operation from the Available Topics menu.**

2. **Select a domain.**

   Highlight the domain you want and press ENTER.

3. **Select Administration.**

4. **Select Real-time Monitor.**

   The Real-time Monitor form is displayed:

   ```
   ┌─────────────────────────────────────────────────────────┐
   │               Real-time Server Monitor Form              │
   ├─────────────────────────────────────────────────────────┤
   │       Direction: Incoming and Outgoing Files             │
   │  File Selection: <Press Insert Key For List>  Scan Type: Secure │
   │  Action Upon Virus Detection: Report Only                │
   └─────────────────────────────────────────────────────────┘
   ```

5. **Enter information on the Real-time Monitor form.**

Press ENTER to display a list of options.

Direction	Description
Incoming files	Files being copied to the domain server and files being opened for writing on the server are considered *incoming* files. Incoming files are scanned after the file is closed.
Outgoing files	Files being copied from the server and files that are being executed from the server are considered *outgoing* files. Outgoing files are scanned when the file is opened. If the file is found to be infected, you will be denied access to it.
Incoming and Outgoing Files	Scans incoming files and outgoing files.
Disabled	Disables the Real-time Monitor.

File Selection

Press INSERT twice to select specific types of DOS and Macintosh files for scanning.

For *DOS files*, you can select all files or a selection of executable files. Since more viruses infect executable files than any other type, you may want to only scan these files. If you select executable files only, you can further define which files to scan by their extensions.

For *Macintosh files*, you can select all files or just application type files or files with a resource fork (the portion of a Macintosh disk file that contains the program code, font information, and other data not normally generated by a user). You can also choose not to scan Macintosh files.

Scan Type

Select one of the following Scan Types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan.* Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Action Upon Virus Detection

Press ENTER to display a list of options. Regardless of which option you choose, a message will be broadcast when a virus is detected

NOTE: InocuLAN's Alert system can be configured to send a message to people in your organization when a virus is encountered. Messages can be sent via pager, e-Mail, FAX, NetWare broadcast, SNMP, or trouble-tickets sent to a printer. This assures that any viral infection on your network is immediately communicated to the people responsible for taking corrective actions. To configure the Alert service, refer to Chapter 4, "Alerting Users If a Virus is Detected."

.

Action	Description
Broadcast	Sends messages via network broadcast, MHS, FAX, SNMP, Trouble Ticket, and Pager, if they have been set up. The message will also appear in the Activity Log.
Delete File	Deletes an infected file from the server.
Rename File	Renames infected files by giving them an AVB extension. Files with this extension will not be scanned by any of InocuLAN's scanners. (See the note below for Macintosh files.) If a file exists with the AVB extension and an infected file in the same directory will result in the same file name, the AVB extension will be changed. The extension will become AV# and the number will be incremented for each subsequent occurrence (AV0, AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory. (See the note below for Macintosh files.)
Purge File	Deletes an infected file so that it cannot be recovered (for example, using Novell's Salvage utility).
Move and Rename File	Renames infected files by giving them an AVB extension and moving them to the INOCULAN\VIRUS directory. (See the note below for Macintosh files.)

NOTE: An infected Macintosh file cannot be renamed or moved.

Every Macintosh file has a file type. If a virus is found, the file type is changed to prevent the file from being used and prevent the virus from spreading. The file types are:

Macintosh File Type	New File Type
Application - APPL	INOA
Data - DATA	INOD
Resources - RSRC	INOR
Stack - STAK	INOS
Text - TEXT	INOT

6. Press F2 when the form is complete.

7. Answer **Yes** to confirm.

   The real-time scanning configuration will take effect immediately.

Recovering from a virus

If the Real-time monitor finds a virus, you must begin proper virus recovery procedures. See Chapter 11, "Virus Recovery Procedures," for details.

Using IMMUNE

IMMUNE is a TSR that scans files on your workstation for viruses each time a file is executed, accessed, or opened. It can be set to monitor your workstation for virus-like behavior, such as unauthorized formatting of your hard disk. IMMUNE can detect known and unknown viruses.

There are three versions of IMMUNE:

➣ Small - uses 11-13 K conventional memory

➣ Medium - uses 30 K conventional memory

➣ Large - memory usage varies depending upon where IMMUNE is loaded:

➣ Loaded in conventional memory uses 109 K conventional memory.

➣ Loaded in extended memory uses 7 K conventional memory and 125 K extended memory.

➣ Loaded in expanded memory uses 7 K conventional memory, 61 K extended memory, and 64 K expanded memory.

The large version detects more viruses than the small and medium versions, but uses more memory. The large version detects all of the viruses listed in the Virus List (available through the InocuLAN for DOS Manager).

You can specify which version of IMMUNE you want to use when you load IMMUNE. There are also a number of options you can use when loading IMMUNE. They are discussed on page on page 9-19.

If IMMUNE finds an infected file, a window will pop up on your screen to inform you. The message will display the name of the infected file and the name of the virus.

> NOTE: IMMUNE will not scan files coming from a server that has real-time scanning enabled. Viruses will be reported by the Real-time Monitor.

Loading IMMUNE

IMMUNE can be loaded from a public directory on a file server or from a workstation. It can be loaded through a workstation's AUTOEXEC.BAT, when a login script is executed, or it can be loaded manually.

Using the
AUTOEXEC.BAT

When InocuLAN for DOS is installed on a workstation, IMMUNE is copied to InocuLAN's home directory (where InocuLAN for DOS is installed). If the workstation's AUTOEXEC.BAT is modified during the installation, IMMUNE will be loaded each time the workstation is booted.

If the AUTOEXEC.BAT was not modified but you want to use it to load IMMUNE, you will have to add a command to the AUTOEXEC.BAT. The command must specify the path where IMMUNE is located. For example, if your InocuLAN for DOS home directory is the INOCULAN directory on your C drive, your statement would look like the following:

```
C:\INOCULAN\IMMUNE.EXE
```

Using login scripts	If you want to use login scripts to load IMMUNE, you will have to add a command to the system login script or to each user's login script. The command must specify the path where IMMUNE is located. You must also have the statement EXIT "IMMUNE" as the last statement in the login script.
Manually loading IMMUNE	You can manually load IMMUNE from a DOS prompt. If you do this, each time the workstation is rebooted, IMMUNE will have to be manually loaded again.
Loading IMMUNE on a workstation without InocuLAN	If a workstation does not have InocuLAN installed, you can still load IMMUNE. The only files needed to run IMMUNE are:

> `IMMUNE.DAT`
> `INMEM.DAT`
> `IMMUNE.EXE`
> `MIMMUNE.DAT`
> `SIMMUNE.DAT`

Loading IMMUNE on an OS/2 workstation	IMMUNE must be loaded in a DOS box on an OS/2 workstation. Each time you open a DOS box, you must load IMMUNE. This can be done automatically by adding a command to the AUTOEXEC.BAT. The command must specify the path where IMMUNE is located.
Loading IMMUNE without any options	**The command to load IMMUNE is:**

1. Type IMMUNE.

Be sure to specify the correct path for IMMUNE.

IMMUNE's defaults

If you do not specify any options when you load IMMUNE, it will be loaded with its defaults. The defaults are:

➢ The large version of IMMUNE is loaded

➢ IMMUNE is loaded into expanded memory (if available)

➢ IMMUNE is loaded with network communication features

➢ 640 K of memory will be scanned

➢ Only executable files will be scanned

IMMUNE's options

There are several options you can use with IMMUNE. To load IMMUNE with options:

1. Type `IMMUNE /option1 /option2`.

Be sure to specify the correct path for IMMUNE.

You can specify one or more options. The options are described in the following table:

Option	Description
/ALL	Scans all files (not just executable files).
/DIS	Disables IMMUNE without unloading it.
/ENA	Enables IMMUNE (if it is disabled).
/H or /?	Displays help.
/HNG	Locks the workstation if a virus is found. This will prevent users from ignoring a virus message. If a virus is found, the workstation will have to be rebooted before proceeding. *Be aware that any unsaved information in open files will be lost!*
/LC	Installs the large version of IMMUNE in conventional memory.

Option	Description
/LE	Installs the large version of IMMUNE in expanded memory. About 7 K of conventional memory will also be used.
/LX	Installs the large version of IMMUNE in extended memory. About 7 K of conventional memory will also be used.
/M	Installs the medium version of IMMUNE.
/N	Does not scan memory.
/NFS	Completely scans files. Without this option, IMMUNE only checks the beginning and end of data files. Executable files (*.EXE, *.COM, etc.) are always fully scanned. This option requires a large amount of CPU resources.
/NOP	Does not scan files that are open.
/NT	Returns an errorlevel of 1 if IMMUNE is not loaded. (This option can be used in a batch file or system login script.) See the next page for more information.
/NTC	Updates the virus signature file if it is out of date.
/NTL	Returns an errorlevel of 1 if the large version of IMMUNE is not loaded. (This option can be used in a batch file or system login script.) See the next page for more information.
/PR	Monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk.
/XEN	Removes Enforcement management for your workstation. Use if your workstation does not log in to an InocuLAN domain server. For memory management purposes, this option removes the Enforcement capability from IMMUNE. This option is solely for stand-alone environments.

Option	Description
/XHK	Does not rehook interrupt 21 for DOS. Use if you have other TSRs that consistently rehook to this interrupt. Use this option if you .are having a problem with IMMUNE and another TSR
/XLN	Disables all network communication features. Use for stand-alone workstations. Reduces the size of IMMUNE.
/Q	Does not display messages while IMMUNE is loading.
/S	Loads the small version of IMMUNE.
/U	Unloads IMMUNE from memory. If a TSR is loaded after IMMUNE, IMMUNE will not unload.
/1	Scans 1 Meg of memory.

Using the /NT or the /NTL option in a DOS batch file

The /NT and the /NTL options can be used in a DOS batch file to notify users whether or not IMMUNE is loaded.

The following example shows you how you can add the /NT option to a batch file:

```
Echo off
IMMUNE /NT
If errorlevel 1 goto one
If errorlevel 0 goto zero
Echo Other value
Goto Exit
:one
Echo IMMUNE is not loaded or IMMUNE was
  deactivated
Goto Exit
:Zero
ECHO IMMUNE is active
:Exit
```

Using the /NT or the /
NTL option in the
system login script

The following example shows you how you can add the /NT option to the system login script:

```
REM assuming IMMUNE.DAT and IMMUNE.EXE are
in
REM SYS:INOCULAN
#sys:\inoculan\immune /nt
if "%ERRORLEVEL"=="10" then  write "immune
   not loaded or inactive"
if "%ERRORLEVEL"=="0" then write "immune
   active"
```

Recovering from a virus

If the Real-time monitor finds a virus, you must begin proper virus recovery procedures. See Chapter 11, "Virus Recovery Procedures," for details.

Using Enforcement

Enforcement adds more security to your network by preventing viruses from being copied to an InocuLAN server. It does this by forcing users to have IMMUNE loaded and active before they can log in to the server.

If a user tries to log in to the server without having IMMUNE loaded, messages will be sent to the user informing him or her to load IMMUNE or be disconnected. The amount of time during which the user will receive these messages is called the grace period. The default grace period is 60 seconds, which can be modified using the Domain Manager.

Enforcement is not active initially

When InocuLAN is first installed, the Enforcement option is not active. All users are allowed to log in to the domain server. You should activate Enforcement once users have access to IMMUNE.

Activating Enforcement

Enforcement can only be activated if the InocuLAN Server is loaded.

Do the following to activate Enforcement:

1. **Select Domain Operation from the Available Topics menu.**

2. **Select a domain.**

    Highlight the domain you want and press ENTER.

3. **Select Administration.**

4. **Select Activate Enforcement.**

    A confirmation screen appears.

5. **Select YES.**

The *Activate Enforcement* menu option will change to *Deactivate Enforcement*.

NOTE: Workstations without IMMUNE loaded and active will be disconnected after Enforcement is activated and the grace period elapses.

Excluding users and groups from Enforcement

InocuLAN for DOS allows certain users, groups and workstation addresses to be exempt from Enforcement. This may be necessary for certain remote users or workstations that do not have enough memory for IMMUNE.

As a default, the user "Supervisor" is excluded from Enforcement. If other people tend to use the Supervisor's ID, you may want to remove it from exclusion. Your Enforcement list will be shared by all members of the domain.

To include or exclude users, groups and workstation addresses from Enforcement:

1. Select Domain Operation from the Available Topics menu.

2. Select a domain.

   Highlight the domain you want and press ENTER.

3. Select Administration.

4. Select Enforcement List.

   A list of currently excluded users and groups appears:

Supervisor will be listed the first time this list is displayed.

```
┌──────────────────────────────────────────────────┐
│          Exclude Users/Groups From Enforcement     │
├──────────────────────────────────────────────────┤
││USER │ SUPERVISOR                                 ││
││     │                                            ││
││     │                                            ││
││     │                                            ││
││     │                                            ││
││     │                                            ││
││     │                                            ││
└──────────────────────────────────────────────────┘
```

The Enforcement screen allows you to configure enforcement in two ways: by building a list of Users and Groups and then deciding if you want to Exclude or Include them.

5. Press INSERT.

   A list of users and groups who are not excluded appears:

```
┌──────────────────────────────────────────────────┐
│                 Users Under Enforcement            │
├──────────────────────────────────────────────────┤
││GROUP│ EVERYONE                                   ││
││USER │ ALERT_SVR00438576                          ││
││USER │ CHEY_USVR                                  ││
││USER │ ELLEN                                      ││
││USER │ GUEST                                      ││
││USER │ KENDALL                                    ││
││USER │ NAOMI                                      ││
││     │                                            ││
││     │                                            ││
││     │                                            ││
└──────────────────────────────────────────────────┘
```

6. Highlight the users or groups you want to exclude or include.

   To select several users or groups, mark each with the F5 key.

7. If you wish to enter a workstation address, press Insert and enter the address.

   A workstation address is useful for Enforcement purposes, because it will let you subject a *particular*

machine to Enforcement, no matter what user has logged on using that machine. You can repeat the process to enter as many addresses as needed.

The workstation address is the 12-character node address, such as: `0000c08aed99`.

8. Press ENTER.

   The list of excluded users and groups appears.

   You now have the option of switching the list of users, groups and addresses from *Exclude* to *Include* by pressing the F4 key. This will toggle the window from *Include Users/Groups* to *Exclude Users/ Groups*.

9. Press F4 as needed to set the user list to Include in Enforcement or Exclude From Enforcement.

10. Press F2 to save the list.

11. Answer **Yes** to confirm.

Deactivating Enforcement

To deactivate Enforcement:

1. Select Domain Operation from the Available Topics menu.

2. Select a domain.

   Highlight the domain you want and press ENTER.

3. Select Administration.

4. Select Deactivate Enforcement.

   A confirmation screen appears.

5. Select **YES**.

   The *Deactivate Enforcement* menu option will change to *Activate Enforcement*.

Changing the grace period for Enforcement

You can change the grace period for Enforcement. To do this:

1. Select Domain Operation from the Available Topics menu.

2. Select a domain.

Highlight the domain you want and press ENTER.

3. Select Administration.

4. Select Server Configuration.

5. Enter a new value in the Enforcement Grace Period field.

Values are entered in seconds. The default grace period is 60 seconds.

Server Configuration

InocuLAN allows you to configure a number of server functions through the Domain Manager.

To configure the server:

1. Select Domain Operation from the Available Topics menu.

2. Select a domain.

3. Select Administration.

4. Select Server Configuration.
   The following options are available:

Automatic Update Enabled	When selected, InocuLAN will automatically synchronize all of your InocuLAN domain servers with the most current version of InocuLAN's virus signature files.
Send Alert to Local Server	If the server is a member of a domain, entering YES will send alerts to the server, as well as to the master server.
NCOPY delay	Enter the number of milliseconds that the Real-time Monitor should wait before scanning files copied with NCOPY.
Enforcement Grace Period	Specifies the amount of time a user has to load WIMMUNE before being disconnected from the server. For more information, see 'Using Enforcement' on page on page 9-23.
Completed Job Hold Time	Specifies the time that a completed job will remain in the Job Queue record. The values entered may be between 1 and 30 days.

Scan Queue Poll
Interval

Specifies the time that passes between each check of the scan queue. When the scan queue is checked, updated information is passed to the Domain Manager. The values entered may be between 1 and 60 seconds.

Viewing Workstation Scanning Records

The Domain Manager allows you to view the
workstation scanning records of all users logged in to
the domain. In order to generate workstation records,
one of two criteria must be present:

> ➤ The InocuLAN Manager is installed on
>   the server, and not on the workstation.
> ➤ The AVUPDATE function is used with
>   the U option. (See the InocuLAN
>   AntiVirus For NetWare AntiVirus
>   Manual for details.)

To view workstation scanning records from the Domain
Manager:

1. Select Domain Operation from the Available Topics menu.

2. Select a domain.

3. Select View Workstation Scanning Records.

    The Workstation Scan Record window appears:

Click here to
access the
individual
workstation
scanning record.

Machine Name	Last Login User Name	Critical	Warning	Infomational
00000102-0000c08aed99	ELLEN	7	2	6
00000102-0000c0920880	ELLEN	2	2	8

The scan summary is listed by machine name and
user login name. The number of Critical, Warning
and Informational messages in each scan record is

shown. A Critical message may mean a workstation has a virus.

4. Click on a workstation entry to access the workstation scanning record.

```
Execution Time   Source 00000102-0000c08aed99      Action    Virus  Status
12-05-95 10:54am C:\                             Cure File      0 Canceled
11-29-95 03:56pm T:\                             Cure File      0 Canceled
11-29-95 10:12am A:\                             Cure File      1 Complete
11-29-95 10:11am A:\                             Cure File      2 Complete
11-29-95 10:11am A:\                             Cure File      3 Complete
11-29-95 10:10am A:\                             Cure File      1 Complete
11-29-95 10:09am A:\                             Cure File      0 Complete
11-29-95 10:09am A:\                             Cure File      0 Complete
11-29-95 10:09am A:\                             Cure File      1 Complete
11-29-95 10:08am A:\                             Cure File      0 Complete
11-29-95 10:08am A:\                             Cure File      1 Complete
11-29-95 10:08am A:\                             Report Only    1 Complete
11-29-95 10:07am A:\                             Report Only    0 Complete
11-29-95 10:07am A:\                             Report Only    0 Complete
11-28-95 09:27am T:\                             Report Only    0 Complete
```

You can easily see the scans that reported a virus or a Critical message.

5. Click on a selected record to view scan detail details.

```
Cheyenne InocuLAN for Windows

Report For Scan Executed On  11/29/95  At 10:11 AM

Drive Scanned              : A


Total Boot Virus Infections   : 1
Total Boot Infections Cured   : 1

Total Directories Scanned     : 1
Total Files Scanned           : 13
Total Viruses Found           : 3

Total Files Infected          : 2
Total Files Cured             : 2
Total Files Deleted           : 0
Total Files Purged            : 0
```

Protecting Your Critical Disk Area

The Critical Disk Area of a workstation includes the Master Boot sector, Partition Table, CMOS RAM information (system configuration information for your AT or compatible computer), I/O System file, DOS system file, and Shell file (the COMMAND.COM in DOS).

The Critical Disk Area of a floppy contains the Boot sector. If the floppy is a bootable diskette, the Critical Disk Area also includes the I/O system file, DOS system file, and Shell file.

It is very important to maintain a current set of Critical Disk Area files for all workstations.

After installation of the InocuLAN for DOS Manager, you should take a moment to back up the Critical Disk Area of your workstation to a rescue diskette. In addition, this area is backed up to the InocuLAN for DOS home directory (the directory in which InocuLAN for DOS was installed).

Through InocuLAN for DOS, you can make a new backup of your Critical Disk Area, examine the area for viruses and changes, and restore the area from a backup.

Back Up your Critical Disk Area

Use *Back Up* to create a rescue diskette for a workstation. The diskette you use as a rescue diskette should be a DOS system diskette. The CONFIG.SYS on this diskette must have FILES=40 or a higher number.

You should back up your Critical Disk Area
immediately after installing InocuLAN, anytime you
change your CMOS information, change your hard disk,
or upgrade your operating system.

To back up your Critical Disk Area:

1. Select Protect Critical Disk Area from the Available Topics
    menu.

2. Select Back Up from the Critical Area Options menu.

3. Select a destination from the list.

4. Press ENTER.

    The Back Up Activity screen will appear and the
    back up will begin.
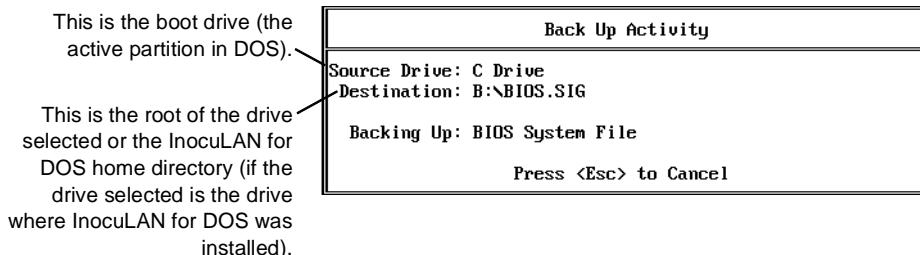
This is the boot drive (the
active partition in DOS).

This is the root of the drive
selected or the InocuLAN for
DOS home directory (if the
drive selected is the drive
where InocuLAN for DOS was
installed).

```
┌──────────────────────────────────────────────┐
│                Back Up Activity                │
├──────────────────────────────────────────────┤
│ Source Drive: C Drive                          │
│ Destination: B:\BIOS.SIG                       │
│                                                │
│  Backing Up: BIOS System File                  │
│                                                │
│            Press <Esc> to Cancel               │
└──────────────────────────────────────────────┘
```

The information that is backed up and the files that are created are listed below:

Information	File
CMOS settings	CMOS.SIG
Partition table	PARTSECT.SIG
Boot sector	BOOTSECT.SIG
DOS system file	DOS.SIG
DOS shell file	SHELL.SIG
BIOS system file	BIOS.SIG
AUTOEXEC.BAT file	AUTOEXEC.SIG
CONFIG.SYS file	CONFIG.SIG
Information about the above files and their location on the hard disk	INFO.SIG

Examine your Critical Disk Area

Use *Examine* to check your local bootable drives for viruses. Examine compares your Critical Disk Area with an existing backup.

To examine your Critical Disk Area:

1. **Select Protect Critical Disk Area from the Available Topics menu.**

2. **Select Examine from the Critical Area Options menu.**

3. **Select the drive to be examined.**

4. **Press ENTER.**

   The Examine Activity screen will appear and the examination will begin.

   If a virus or change is detected in the Critical Disk Area you can use a rescue diskette to restore the

area. (First check to see if there is a reason for a change in the area, such as a new version of DOS.)

Restoring your
Critical Disk Area

Use *Restore* to recover from an infection or corruption of the Critical Disk Area.

NOTE: **If you have a serious infection that will not allow you to boot your machine from the hard drive, see 'Critical Disk Area Lost' in Chapter 11, "Virus Recovery Procedures," for instructions.**

To use the Restore function:

1. **Select Protect Critical Disk Area from the Available Topics menu.**

2. **Select Restore from the Critical Area Options menu.**

3. **Select the drive from which you want to restore.**

   The best place to restore from is a rescue diskette. If you do not have one, select the backup from the file server. Your last choice should be from your local hard drive.

4. **Press ENTER.**

   The Restore Activity screen will appear and the restoration will begin.

Using the EXAMINE utility

EXAMINE is a command line utility that checks your workstation's hard disk for boot viruses. Your workstation's Critical Disk Area is examined for changes, including infection and corruption. The Critical Disk Area includes the boot sector, partition table, CMOS RAM information, and DOS system files. EXAMINE also lets you back up and restore your Critical Disk Area. (These functions are also available through the DOS Manager. See 'Protecting your Critical Disk Area' on page on page 9-32.)

Running EXAMINE   You can run EXAMINE by doing the following:

1. Type EXAMINE at the DOS prompt.

Be sure to specify the correct path for EXAMINE.

If you want to be able to run EXAMINE from any directory, your AUTOEXEC.BAT should include the InocuLAN for DOS home directory (the directory where InocuLAN for DOS is installed) in its path. If you allowed your AUTOEXEC.BAT to be modified during installation, this was done for you. If you did not, you must add the following statement to your AUTOEXEC.BAT:

```
SET INOCULAN=path
```

where 'path' is your InocuLAN for DOS home directory. For example, if your InocuLAN for DOS home directory is the INOCULAN directory on your C drive, your statement would look like the following:

```
SET INOCULAN=C:\INOCULAN
```

EXAMINE's options   There are several options you can use with EXAMINE.

To load EXAMINE with options:

1. Type **EXAMINE /option** at a DOS prompt.

    Be sure to specify the correct path for EXAMINE.

    The options are described in the following table:

Option	Description
/A	Accepts changes. If the Critical Disk Area has changed, this option updates the signature files.
/C	Creates new backup files that can be used to restore in the event of infection or corruption.
/H or /?	Displays help.
/I	Ignores changes. If the Critical Disk Area has changed, this option does not update the signature files.
/L	Uses the local (home) directory, not the directory specified in the environment variable.
/N	Does not scan memory.
/Q	Quiet mode. EXAMINE will run without being seen by the user.
/R	Restores the Critical Disk Area if it has changed.
/S	Does not check CMOS RAM information.
/1	Scans 1 Meg of memory. (The default scans 0-640K.)

EXAMINE is automatically run each time you boot
your computer. This offers extra protection because
your memory is scanned before other programs are
loaded, thereby preventing a virus from spreading.

EXAMINE is run by the following statement that is
added to your AUTOEXEC.BAT file during
installation:

C:\INOCULAN\EXAMINE

You may add any of the EXAMINE options to this
statement.

Keeping your InocuLAN system up-to-date

Part of the process of safeguarding your network against
viruses involves keeping your InocuLAN system up-to-
date with the latest software available.

For details on updating InocuLAN, see 'Keeping your
InocuLAN system up-to-date' on page 3-37.

10

C h a p t e r

INOCULAN FOR MACINTOSH

This chapter provides you with an overview of InocuLAN for Macintosh.   It also tells you how to install and use it.

In this chapter, you will learn:

About InocuLAN for Macintosh

What is InocuLAN for
Macintosh?

InocuLAN for Macintosh is a virus protection program that decontaminates and protects your Macintosh against known computer viruses. The InocuLAN for Macintosh application detects contaminated files, removes the virus and reverses any side effects, repairing the file.

InocuLAN for Macintosh consists of two primary pieces, the application program and the InocuLAN INIT. The application is what you run first, before doing anything else, to check for and remove viruses from your hard disk.

After you've "cleaned" your disk, you can place the INIT in your system extension folder. Once the InocuLAN INIT is active, any attempt to run a program contaminated with a known virus will result in a system error indicating that the file is already open. This will prevent the contaminated application from opening and spreading the virus.

Installing InocuLAN for Macintosh

This section provides you with the basic instructions for installing InocuLAN on the Macintosh. You will create diskettes that you can use to install InocuLAN on the Macintosh. Do not try to insert the ManageWise CD on the Macintosh and install the InocuLAN software directly from the CD to the Macintosh.

To Create the Macintosh disks,

1. Insert the ManageWise CD into the CD-ROM drive.

2. Select Run from the Windows 95 Start menu. Browse the ManageWise 2.5 CD until you see the following path:

    \InocuLAN\clients\mac\disk1\inomac.exe

3. A DOS box will come forward titled: INOMAC and will request the following:

    InocuLAN ver 2.5 for MAC Install disk

4. Insert a blank high-density diskette in drive A. Press enter to extract, or ESC to exit.

5. Place a blank floppy into drive A and the diskette will be formatted into MAC O/S and the installation and program files copied to the diskette

    The InocuLAN for MAC diskette can then be used to install directly onto a Macintosh computer.

    The contents of the InocuLAN for MAC diskette can be copied to the Macintosh volume on a NetWare server ad the installer run by Macintosh users on demand.

The InocuLAN for Macintosh application requires
System software 6.0 or higher and 128K or 256K ROMs
(these are the ROMs used in the Mac Plus, SE, II and
above).

> **NOTE:** **Do not attempt to run this software with earlier System
> versions or on machines with 64K ROMs.**

The InocuLAN for Macintosh application is fully
MultiFinder compatible and will run in the background
under MultiFinder.

To install the InocuLAN for Macintosh application:

1. Insert the InocuLAN diskette into a disk drive.

**2. Copy the InocuLAN files to the hard disk by dragging the
InocuLAN disk to your hard disk.**

> **NOTE:** **You must keep the InocuLAN program and associated
> files in the Cheyenne folder for the INIT to work
> properly.**

**3. Open the InocuLAN folder (on your hard disk) by double
clicking on it.**

You will see the following files:

4. Scan your hard disk for viruses.

See the following section 'Quick Start: Scanning
your hard disk for viruses' for information about
checking your hard disk.

Quick Start: Scanning Your Hard Disk for Viruses

To quickly get started protecting your Macintosh, here is the minimum information necessary to use InocuLAN for Macintosh.

1. Start the InocuLAN for Macintosh application.

   Open the folder you installed on your hard disk and double-click the InocuLAN icon.

2. Select Repair Volume/Folder... from the File menu.

File	
Repair Volume/Folder...	⌘F
Repair File...	⌘O
Close	⌘W
Save As...	⌘S
Quit	⌘Q

3. Select your normal startup volume (your hard disk) and click the Select button to check/repair it.

   ```
   ☰ Desktop ▼
   🖳 InocuLAN            ⬆        ⬦ Quadra
      Quadra
   ⊞ WRITER2.SYS
                                  ( Open )
                                  ( Select )
                          ⬇       ( Cancel )
   ```
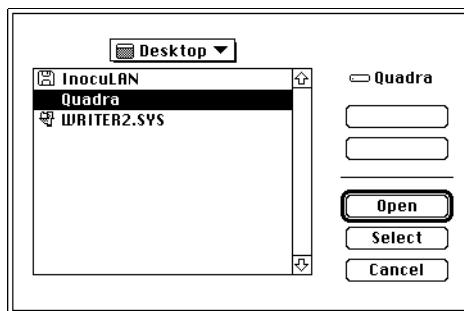
   If you get an error from InocuLAN, such as "The file 'Word' is busy and could not be examined", try closing the file (or application) that was busy and checking it again.

4. Drag the InocuLAN INIT into your System Folder.
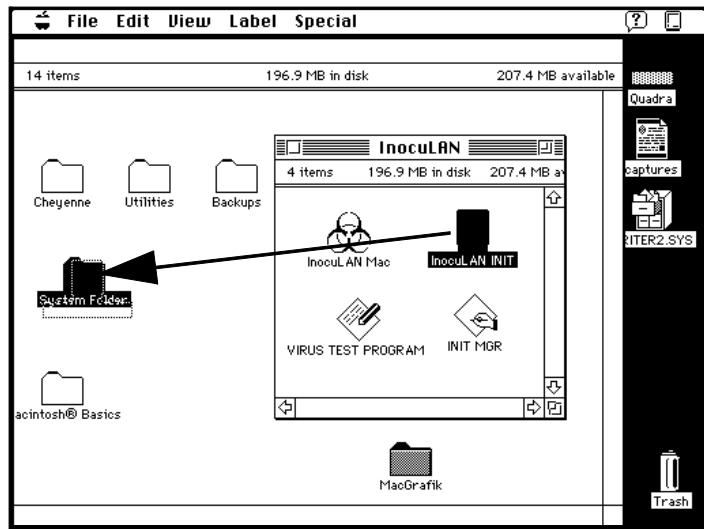
You will get a message telling you that this file must be placed in the Extensions folder. Click OK to put the INIT in the Extensions folder.

5. Restart your computer.

Your disk is now free of all known viruses and the InocuLAN for Macintosh INIT will prevent infection or re-infection by those viruses.

About the InocuLAN for Macintosh INIT

As mentioned before, InocuLAN for Macintosh consists of two primary pieces, the application program and the INIT.

The application is what you run first, before doing anything else, to check for and remove viruses from your hard disk. You should also use InocuLAN to scan diskettes, the first time you use them.

The INIT is copied into your system extensions folder after you've checked and repaired your disk with the InocuLAN for Macintosh program.

The INIT serves three primary purposes:

> ➤ To work in the background scanning files (as you try to execute them) for viruses.
> ➤ To prevent you from opening a file that is infected with a virus.
> ➤ To notify you through Alert.NLM when a virus is detected (if you have mounted a NetWare volume that is running the DOS/NetWare version of InocuLAN).

Receiving alert messages through a NetWare server

Alert is a program that runs on a NetWare server. It works with the InocuLAN.NLM to alert you of virus infections. Alert can inform you of virus infections using a number of methods including sending you a FAX, paging you, and sending you E-mail.

Again, you must have mounted a NetWare volume on your Macintosh that is running InocuLAN for DOS and Alert in order for INIT to notify you of viruses through the NetWare server.

If you try to run or open an infected file after you've installed the INIT in your system folder, a message similar to one of the following will appear:

Typical message displayed by the finder when you try to use an infected file

```
┌─────────────────────────────────────────────────────┐
│ ┌─────┐   The following application is busy or damaged:│
│ │     │   Word Processor                                │
│ └─────┘                                                 │
│                                                         │
│ ┌─────────┐                                             │
│ │ Finder  │                                             │
│ └─────────┘                                             │
└─────────────────────────────────────────────────────┘
```
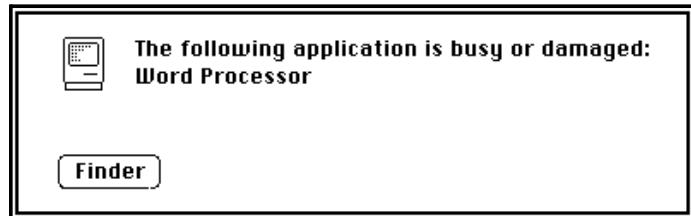
Typical message displayed by MultiFinder when you try to use an infected

```
┌─────────────────────────────────────────────────────┐
│  ┌───┐      The file "Drawing Program" could not      │
│  │   │      be opened/printed (the file is busy).     │
│  └───┘                                                 │
│                                                        │
│  ┌────────┐                                            │
│  │   OK   │                                            │
│  └────────┘                                            │
└─────────────────────────────────────────────────────┘
```
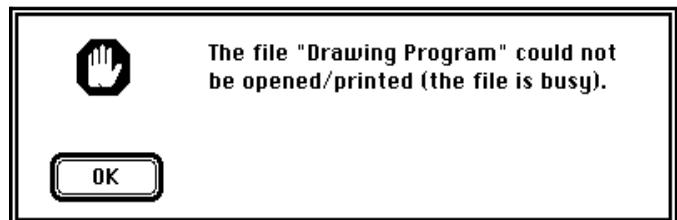
After you close the above dialog boxes, you should get another dialog box that gives you more details about the virus that has infected the file:

```
┌─────────────────────────────────────┐
│  ┌─────────────────────────────┐     │
│  │  ✋  The 'nVIR' virus was    │     │
│  │      detected in file 'VIRUS │     │
│  │      TEST PROGRAM '          │     │
│  │                              │     │
│  │         [  Alright  ]        │     │
│  └─────────────────────────────┘     │
└─────────────────────────────────────┘
```

Again, the InocuLAN for Macintosh INIT acts to prevent contamination by known viruses by generating a system error, indicating that a contaminated application is already open. This prevents the infected file from opening and the contamination from spreading, defeating the virus.

STOP

Immediately check any program that causes an "already open" error alert with the InocuLAN for Macintosh application.

Repairing Volumes and Folders

Follow these directions to check and repair an entire hard disk or folder:

1. Start InocuLAN for Macintosh by double clicking on the InocuLAN application icon.

   The InocuLAN splash screen will appear. Click anywhere on the splash screen to continue. Your desktop should look similar to the following:

   This icon indicates that InocuLAN is running.
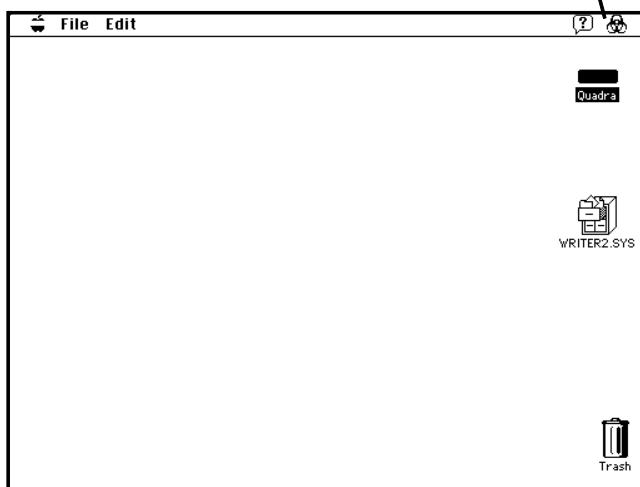
2. Select Repair Volume/Folder... from the File menu.

```
File
Repair Volume/Folder...    ⌘F
Repair File...             ⌘O

Close                      ⌘W
Save As...                 ⌘S

Quit                       ⌘Q
```

A dialog box similar to the following appears:

```
                 🖳 Desktop ▼

💾 InocuLAN                ⬆        ⬡ Quadra
   Quadra
🦟 WRITER2.SYS
                                   ┌──────────┐
                                   │          │
                                   └──────────┘
                                   ┌──────────┐
                                   │          │
                                   └──────────┘

                                   ┌──────────┐
                                   │   Open   │
                                   └──────────┘
                                   ┌──────────┐
                          ⬇        │  Select  │
                                   └──────────┘
                                   ┌──────────┐
                                   │  Cancel  │
                                   └──────────┘
```
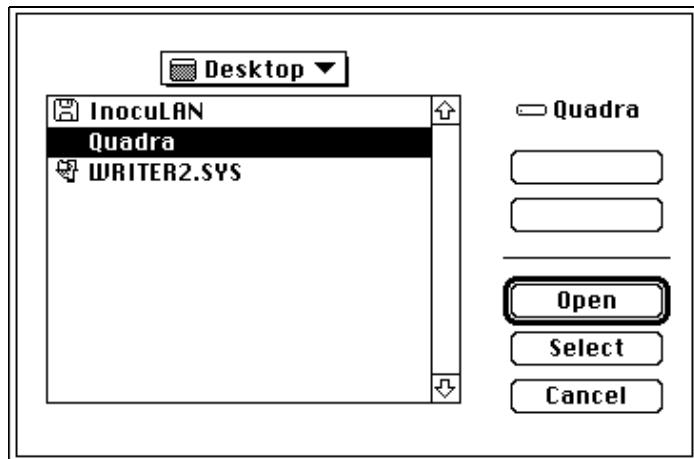
3. Select the volume (disk) or folder that you want to process and click "Select".

   The InocuLAN for Macintosh application window shown below opens:

```
▤▫═══════════ After Dark Files ═══════════▫◪
┌─Files──┐┌─Infected┐┌─Repaired┐┌─Errors─┐
│ 00007  ││ 00000   ││ 00000   ││ 00000  │ InocuLAN Mac v2.2
└────────┘└─────────┘└─────────┘└────────┘
Checking "Clock"...
```

There are four counter fields:

- ➤ Files
- ➤ Infected
- ➤ Repaired
- ➤ Errors

To the right of the counter fields, a field displays the version number of InocuLAN for Macintosh. Always refer to this version number when contacting Cheyenne. Just below the counter fields, there is a field that displays the names of files as they are checked.

> NOTE: You can stop InocuLAN for Macintosh at any time, in both check and repair modes, by pressing the command and period keys together.

The "Files" counter shows the number of files checked by InocuLAN for Macintosh. The "Infected" counter shows the number of infected files found and the "Repaired" counter shows the number of files that have been repaired by removing the viruses that had infected them. At the end of a successful InocuLAN for Macintosh run, the "Infected" and "Repaired" counters will always be equal.

The "Errors" counter shows the number of files that could not be checked or repaired because of an operating system condition such as "File Open". If you get a "File Open" error, close the file and check it again.

NOTE: Note that all the counters show the number of files infected, repaired, or having an error reported. Therefore, a file that was infected with more than one virus would be counted only once in "Files", "Infected" and "Repaired". Simultaneous infection of an application by more that one virus is an increasingly common situation. InocuLAN for Macintosh has been designed to handle these cases.

After InocuLAN for Macintosh finishes checking the volume or folder, you can save the status screen (shown on the previous page) as a report. See the section, 'Saving an InocuLAN for Macintosh log as a text file' later in this chapter for more information.

Repairing Individual Files

The Repair File… command is used to process a single file. This is useful for verifying the safety of a new program added after an entire disk has been processed with InocuLAN for Macintosh. Follow these directions to check an individual file:

1. Start InocuLAN for Macintosh.

2. Select Repair File.. from the File menu.

```
┌─────────────────────────────┐
│ File                        │
├─────────────────────────────┤
│ Repair Volume/Folder...  ⌘F │
│ Repair File...           ⌘O │
├─────────────────────────────┤
│ Close                    ⌘W │
│ Save As...               ⌘S │
├─────────────────────────────┤
│ Quit                     ⌘Q │
└─────────────────────────────┘
```

A dialog box similar to the following appears:

```
┌───────────────────────────────────────────┐
│   ☐ System Folder ▼          ⊂⊃ Quadra     │
│ ┌─────────────────────────┐  ┌──────────┐  │
│ │ ☐ After Dark Files    ⇧ │  │          │  │
│ │ ☐ Apple Menu Items    ☰ │  └──────────┘  │
│ │ ☐ AppleLink Out Basket│  ┌──────────┐    │
│ │ ☐ ASMac Data          │  │ Desktop  │    │
│ │ ☐ ASMac Help          │  └──────────┘    │
│ │ ☐ Claris Fonts        │  ┌──────────┐    │
│ │ ☐ Clipboard           │  │ Cancel   │    │
│ │ ☐ Control Panels     ⇩ │  ├──────────┤    │
│ └─────────────────────────┘  │  Open   │    │
│                              └──────────┘    │
└───────────────────────────────────────────┘
```
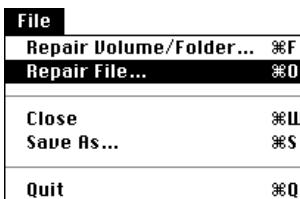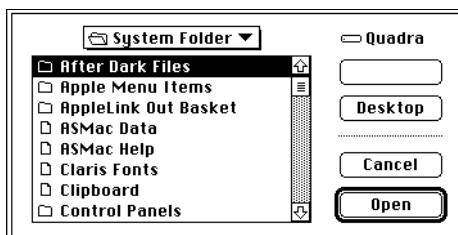
3. Select the file you want to check and click Open.

   InocuLAN for Macintosh scans the file. If the file is infected, it will remove the virus and repair the file. If the file is not infected, a message will appearing telling you this.

Repairing Floppy Disks

Follow these directions to check and repair floppy disks using InocuLAN for Macintosh.

1. Start InocuLAN for Macintosh.

2. Insert a disk in the disk drive.

   Whenever the InocuLAN for Macintosh application is running and active, a floppy disk is automatically processed as soon as you insert it in the disk drive. This has the same effect as selecting the Check Volume/Disk… command.

   As soon as the operation is completed, the disk is ejected. Inserting another disk will start another automatic repair, with a new report window "tiled" over that of the preceding disk. See below:
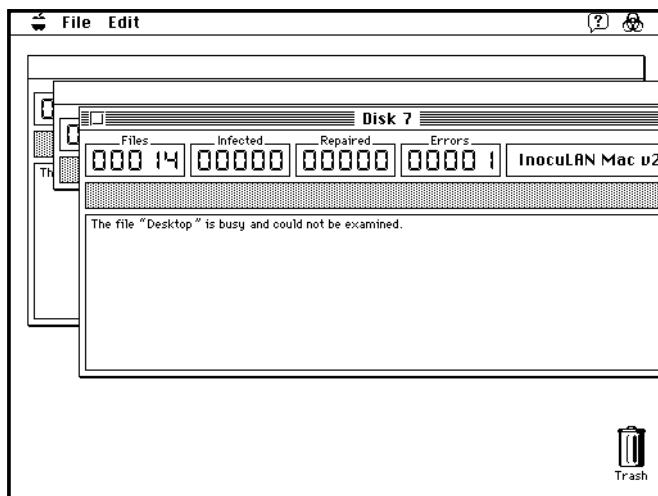
Locked disks   InocuLAN for Macintosh cannot repair locked disks. When a locked floppy disk is inserted the InocuLAN for Macintosh application is running, a message similar to

the following will appear:


```
┌─────────────────────────────────────────────┐
│  ┌───┐    The volume                         │
│  │ ✋ │    "Word Processing" is locked.       │
│  └───┘                                        │
│  ┌─────────┐                                  │
│  │   OK    │                                  │
│  └─────────┘                                  │
└─────────────────────────────────────────────┘
```
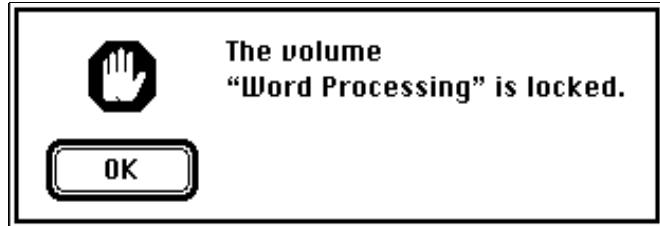
A floppy disk can be unlocked for processing by sliding the write protect tab to the write enable position. A CD-ROM disk, of course, is always locked. See the section, 'Checking Volumes and Files' for information on checking a CD-ROM disk.

Checking Volumes and Files

In normal operation, InocuLAN for Macintosh automatically repairs any contaminated files that it encounters by removing the virus and actively reconstructing damaged parts of the application.

> NOTE: Under some special circumstances, it may be desirable to check a file or volume without automatically repairing (removing) viral infections. For example, checking without repairing may be a first step prior to obtaining permission to repair files.

Another case for simply checking files is checking a CD-ROM disk. CD-ROM disks are always "read only". In the regular InocuLAN for Macintosh repair mode, a CD-ROM will always be a locked disk and InocuLAN for Macintosh will reject it, displaying the following dialog box:

The volume
"Word Processing" is locked.

OK
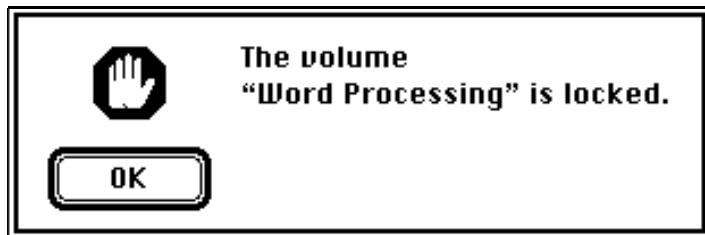
Using the Check Only option of InocuLAN for Macintosh will scan a CD-ROM for viruses, even though a disk of this type can never be repaired.

To use the Check option, follow these directions:

1. Hold down the Option key when pulling down the File menu.

The Repair Volume/Folder… and Repair File… commands will be replaced by Check Volume/Folder… and Check File…, as shown below:

```
File
  Check Volume/Folder...   ⌘F
  Check File...            ⌘O

  Close                   ⌘W
  Save As...              ⌘S

  Quit                    ⌘Q
```

After this, Checking works exactly the same as repairing, that is you select what you want to check and InocuLAN does the rest. See 'Repairing Volumes and folders' and 'Repairing individual files' previously in this chapter for more information about using these options.

Checking diskettes

Diskettes can be automatically checked upon insertion.

To automatically check a diskette on insertion:

1. Hold down the option key when the disk is inserted.

The option key does not have to be held down during the entire check. However, it must be held down whenever a disk is inserted, or that disk will be repaired, rather than checked.

Repairing or Checking AppleShare Servers

You can use InocuLAN for Macintosh to repair or check an AppleShare server. To check an AppleShare server, mount the server volume that you want to repair/check on your Macintosh then select the volume using InocuLAN's Repair Volume/Folder Option.

NOTE: The InocuLAN for Macintosh application can only check those files to which it has access. Therefore, to perform a complete check of a server volume, you must have supervisor or equivalent privileges on the AppleShare server.

You can stop InocuLAN for Macintosh at any time, in both check and repair modes, by pressing the Command and Period keys together.

Using the InocuLAN INIT Manager

The INIT manager (INIT MGR) allows you to enable and disable the InocuLAN for Macintosh INIT. The purpose of the INIT, once it is copied into your System folder, is to prevent you from opening an infected file. There may be times, however, when you absolutely must open an infected file. To do this, you will need to first disable the InocuLAN INIT.

To disable the InocuLAN INIT:

1. Start the INIT MGR.
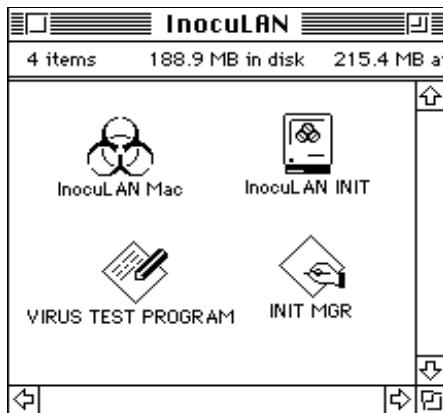
2. Select Disable INIT from the File menu.

   You will now be able to open the infected file.

   The INIT will be disabled for one minute. After one minute, you will hear three beeps which mean the INIT is enabled again.

To enable the INIT:

1. Select Enable INIT from the File menu.

Saving an InocuLAN for Macintosh Log as a Text File

It is often desirable to keep a log of the files that were processed by InocuLAN for Macintosh. The log can be useful in tracing the source, history and consequences of viral infections.

Follow these directions to save a log to a text file:

1. Run repair or check on a volume, file or floppy disk.

2. After the job finishes, select Save As from the File menu.

    A dialog box similar to the following will appear:

```
┌──────────────────────────────────────┐
│        🖫 Startup Disk                │
│  ┌────────────────────┐┌┐ 🖫 Startup Disk │
│  │ 🗀 System Folder    │⇧│                │
│  │ 🗀 Graphics         │ │   ┌────────┐   │
│  │ 🗀 Word Processing  │ │   │ Eject  │   │
│  │ 🗀 Desktop Publishing│ │  ┌────────┐   │
│  │                    │ │   │ Drive  │   │
│  │                    │⇩│                │
│  └────────────────────┘└┘                │
│                                          │
│  Save document as:          ┌────────┐   │
│  ┌──────────────────────┐   │  Save  │   │
│  │ Startup Disk         │   ┌────────┐   │
│  └──────────────────────┘   │ Cancel │   │
└──────────────────────────────────────┘
```
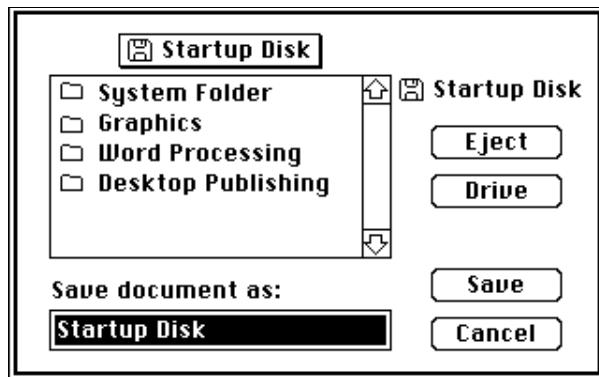
3. Enter a name for this log file and click Save.

    By default, InocuLAN uses the same name as the file/folder that you checked/repaired along with a .txt extension. It also places the file in the folder that you were just checking/repairing.

    You can open or print this text file with any word processor that accepts a text file.

VIRUS RECOVERY PROCEDURES

When a virus strikes, it is vital that you follow proper recovery procedures. This chapter will explain how to recover from various types of virus infections.

In this chapter, you will learn:

What to Do if InocuLAN Discovers a Virus

Required items

You will need the following in order to recover from a virus:

> ManageWise 2.5 CD (and possibly the InocuLAN for DOS Manager diskette).
> A backup of the Critical Disk Area for the infected computer.
> A clean, write-protected, bootable floppy disk containing the operating system files that match the version of the operating system used when the Critical Disk Area was backed up.

It is very important to maintain a current set of Critical Disk Area files for all workstations. This backup may have been created in the following ways:

> A rescue diskette should have been created right after InocuLAN was first installed. The files reside on the rescue disk.
> The backup files were created automatically when an InocuLAN manager was installed and they reside in the InocuLAN home directory.
> EXAMINE /C was run. The files will reside wherever the InocuLAN environment is set.
> The Backup Critical Disk Area option was used. The location of the files is determined by the destination chosen when the backup is made, and can be either a floppy, master server in a

domain, stand-alone server , or local hard
disk. Files backed up to servers are
stored in subdirectories of the InocuLAN
home directory. The subdirectory path is
the network segment followed by the
network interface card (NIC) address.

Infected file detected
or an infection found
in memory

**You should do the following if an infected file is detected or an
infection is found in memory:**

1. **Exit the program you are in (be sure to save your work, if
    necessary).**

2. **Shut off the computer.**

3. **Boot your workstation with a write-protected, virus-free
    boot diskette (such as the original operating system
    diskette).**

    The CONFIG.SYS on this diskette must have
    FILES=40 or a higher number. It is recommended
    that you also add the statement
    DEVICE=HIMEM.SYS. For this statement to
    work, you must copy the HIMEM.SYS file, located
    in the DOS directory, on to the diskette.

    If you do not have a CONFIG.SYS on your diskette,
    you can add the necessary information using the
    following procedure. *Since your own workstation
    may have already been infected, it is highly
    recommended that you do the following at another
    workstation which is infection free.* If no other
    workstation is available, perform the following
    AFTER booting your workstation with the boot
    diskette:

    ➢ At the A prompt, type:

    > **COPY CON CONFIG.SYS   <ENTER>**

   ➢ With the cursor flashing, type:

```
FILES=40
 DEVICE=HIMEM.SYS <F6>  <ENTER>
```

> NOTE: You must disable write-protection to create the
>   CONFIG.SYS file. After creating it, re-enable write-
>   protection on the diskette.

➣ Re-boot your workstation.

4. Run the InocuLAN for Windows Manager or InocuLAN for
   DOS Manager.

5. Use the Local Scanner (in Windows) or Run Scanner (in
   DOS) to scan your hard drive.

   See 'Using the Local Scanner' in Chapter 2 for
   Windows instructions, or 'Using the Run Scanner'
   in Chapter 8 for DOS instructions.

6. Use the scanning report to delete any infected files
   identified (or scan again with the 'Delete File' option) and
   replace the files from a reliable source.

   See 'Checking the results of your scan' in Chapter 2
   for Windows instructions or Chapter 8 for DOS
   instructions.

   The last resort should be to scan with the 'Cure File'
   option selected.

7. Re-scan the hard disk after replacing infected files to
   ensure the virus has been removed from the system.

Boot sector virus
detected or
suspected
(EXAMINE fails)

You should do the following if a boot sector virus is detected or suspected:

1. Cold-boot your workstation with a write-protected, virus-free boot diskette (such as the original operating system diskette).

The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

➢ At the A prompt, type:

    COPY CON CONFIG.SYS   <ENTER>

➢ With the cursor flashing, type:

    FILES=40
    DEVICE=HIMEM.SYS <F6> <ENTER>

NOTE: You must disable write-protection to create the CONFIG.SYS file. After creating it, re-enable write-protection on the diskette.

➢ Re-boot your workstation.

2. Run the InocuLAN for DOS Manager and restore the Critical Disk Area from any of the sources identified in the 'Required items' section.

3. Run EXAMINE to verify that no viruses are found in memory and that the Critical Disk Area has been properly restored.

   See 'Using the EXAMINE Utility' in Chapter 3 for instructions.

Critical Disk Area lost

Depending on the degree of damage, a virus can alter all or part of the critical disk area. If all of the critical disk area is lost, the procedure to recover is as follows:

Restoring from a floppy disk

Be aware that the procedure below asks you to perform the same actions several times. It is important that all these steps are followed as outlined.

To restore from a floppy disk:

1. Cold boot from a clean, write-protected system floppy.

   The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

   If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

   ➣ At the A prompt, type:

      COPY CON CONFIG.SYS   <ENTER>

   ➣ With the cursor flashing, type:

```
FILES=40
 DEVICE=HIMEM.SYS <F6>  <ENTER>
```

NOTE: You must disable write-protection to create the
            CONFIG.SYS file. After creating it, re-enable write-
            protection on the diskette.

➣   Re-boot your workstation.

2. Using the InocuLAN for DOS Manager, restore the Critical
    Disk Area.

    It will report as failed, but CMOS should be
    restored. Boot again from a floppy disk. The
    system should now recognize the existing hard
    drive.

3. Using the InocuLAN for DOS Manager, restore the Critical
    Disk Area.

    It will report as failed, but Partition information
    should now be restored. Boot again from a floppy
    disk.

4. Using the InocuLAN for DOS Manager, restore the Critical
    Disk Area.

    It will report as failed, but the Master boot sector
    should now be restored. Boot again from a floppy
    disk.

5. Using the InocuLAN for DOS Manager, restore the Critical
    Disk Area.

    System files should now be restored. You can now
    boot from your hard drive. All the hard drive
    information should be available. Run CHKDSK to
    verify this. There is a possibility that the virus also
    corrupted part or all of the information on the hard
    drive.

To restore from network:

1. If you haven't already, install the InocuLAN for DOS Manager to a directory on a server.

2. Boot the workstation from a clean, write-protected floppy disk. Include the network drivers (IPX, NETX or equivalent ODI/VLM drivers) on the floppy.

The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

➤ At the A prompt, type:

```
COPY CON CONFIG.SYS    <ENTER>
```

➤ With the cursor flashing, type:

```
FILES=40
DEVICE=HIMEM.SYS <F6>  <ENTER>
```

NOTE: **You must disable write-protection to create the CONFIG.SYS file. After creating it, re-enable write-protection on the diskette.**

➤ Re-boot your workstation.

3. Log in to the server where the Critical Disk Area backup files were made.

4. Change to the directory containing the InocuLAN for DOS Manager files.

5. Run the DOS Manager and restore as per the procedure detailed on the previous page in the 'Restoring from a floppy disk' section.

    Select the name of the server containing the backup files as your source.

A

C h a p t e r

COMMON VIRUS LIST

The information in this appendix describes the symptoms of some of the most common viruses and explains how they infect your computer.

In this chapter, you will learn:

➢ What Symptoms Each Virus Displays

➢ Where do Viruses Come From?

➢ Which Aliases the Virus Uses

➢ How Many Variants (Strains) the Virus Has

➢ How the Virus Infects

➢ What Type of Damage the Virus Causes

Azusa

Aliases: Hong Kong

Type: Resident Boot Sector and Master Boot Sector
Infector

Origin: Hong Kong; February 1991   **Variants**: 1

Overview: Azusa is a memory resident infector of
diskette boot sectors and the hard disk master boot
sector (partition table).

Method of infection: The first time the system is
booted from a diskette infected with the Azusa virus, the
virus will become memory resident at the top of system
memory, but below the 640K DOS boundary.

Symptoms: The CHKDSK command will indicate that
the computer has 1K of memory less than usual.

The virus keeps track of how many times the system has
been booted from an infected diskette. After 32 boots,
the virus will disable the COM1 and LPT1 ports, and
reset its counter. A later boot will result in the ports
functioning properly again.

Damage: Once Azusa is memory resident, it will infect
diskettes when they are accessed on the system with
write intent (for example, a file is opened as output, or
with read/write intent) or when attempting to reboot the
system from a diskette using CTL-ALT-DEL.

When Azusa infects a diskette, it moves the original boot sector to a different address and then copies itself to the original boot sector location. Files may be corrupted, directory entries may be lost, and the disk's FAT may be corrupted.

When Azusa infects the system's hard disk, it overwrites the master boot sector with a copy of the Azusa virus. A copy of the original master boot sector is not saved.

AntiEXE

Aliases: D3, Newbug

Type: Floppy Boot Sector and Master Boot Sector Infector

Origin: 1993   **Variants**: 2

Overview: AntiEXE is a memory resident infector of diskette boot sectors and the hard disk master boot sector (partition table).

Method of infection: The virus fills nearly one sector, moving the Master Boot Sector or Floppy Boot Sector to another location.

Symptoms: If the virus is in memory, a disk viewing tool will show nothing wrong. The CHKDSK command will report 653,312 total bytes of memory, 2,048 bytes fewer than the normal number, 655,360.

Damage: Reduces memory available to DOS by 2K. May overwrite some sectors on diskettes.

Brain

Aliases: Pakistani, Pakistani Brain, Clone, Nipper

Type: Resident Boot Sector Infector

Origin: Pakistan; 1986   **Variants**: 5

Overview: The original Brain virus only infected floppy diskettes. Variants to the virus can now infect hard disks.

Method of infection: The virus is usually transmitted by booting a computer with an infected disk.

The virus installs itself resident in memory, taking up between 3K and 7K of RAM.

Symptoms: Disks infected with the virus will have their volume label changed to "(c) Brain". This label can also be found in sector 0 (the boot sector) on an infected disk. (Some variants of the virus have had this label removed to make them harder to detect.)

Damage: The virus infects disk boot sectors by moving the original contents of the boot sector to another location on the disk, marking those clusters bad in the FAT, and then writing the virus code in the original disk boot sector.

Dark Avenger

Aliases: Amilia, Black Avenger, Boroda, Eddie, Diana, Rabid Avenger, VAN Soft, Dark Avenger 1801, Dark Avenger-C, Dark Avenger-D, PS!KO, Evil Men, Dark Avenger.1E, Dark Quest

Type: Resident.COM and.EXE Infector

Origin: Bulgaria; September 1989   **Variants**: 17

Overview: Dark Avenger is a memory resident virus that infects .COM, .EXE, and overlay files, including the COMMAND.COM. It is extremely good at infecting executable files that are open for any reason, including the DOS COPY and XCOPY commands. Using an infected version of either command to copy uninfected files will result in both the source and target files becoming infected.

Method of infection: The virus becomes memory resident when the system is booted with an infected disk.

Symptoms: Infected files will have their lengths increased by 1,800 bytes.

Damage: The Dark Avenger virus maintains a counter in the disk's boot sector. After each sixteenth file is infected, the virus will randomly overwrite a sector on the disk with a portion of the Dark Avenger virus code. If the randomly selected sector is a portion of a program or data file, the program or data file will be corrupted. Programs and data files which have been corrupted by a sector being overwritten are permanently damaged and cannot be repaired since the original sector is lost.

Exebug

Aliases: CMOS, CMOS Killer

Type: Floppy Boot Sector and Master Boot Sector Infector

Origin: 1993, South Africa **Variants**: 2

Overview: Exebug will alter the CMOS setup to not read from a floppy drive. This prevents booting from a clean system diskette because the virus loads itself from the hard drive *before* the system will attempt to boot from a diskette.

Method of infection: Infects hard disks when booting from infected floppies.

Symptoms: May produce message "Drive A: not installed" when booting.

Damage: Exebug generates a disk-trashing virus on hard drive. On floppies, it converts sectors into virus-droppers.

FORM-Virus

Aliases: Form, Form Boot, FORM-18

Type: Resident Boot Sector Infector

Origin: Switzerland; June 1990   **Variants**: 3

Overview: FORM-Virus is a memory resident infector of floppy and hard disk boot sectors.

Method of infection: The virus is usually transmitted by booting a computer with an infected disk.

Symptoms: Systems infected with the FORM-Virus in memory may notice a clicking noise being emitted from the system speaker on the 24th day of any month.

Damage: When a system is booted with a diskette infected with the FORM-Virus, the virus will infect system memory as well as seek out and infect the system's hard disk. The floppy boot may or may not be successful.

Freddy

Aliases: Brasil, Freddy.2

Type: Infects COM and EXE files, COMMAND.COM and IBMBIO.COM

Origin: 1990, Indonesia   **Variants**: 2

Overview: A dangerous and clever virus that hides in memory. Effects of Freddy may be activated by system date.

Method of infection: Virus contains code that searches for COM and EXE files, then links to any location within the file. Virus will infect software during a program load, then restart the software after modifications are made.

Symptoms: The word Freddy appears in a box on the screen.

Damage: Will erase data by doing an absolute write to one or more sectors on a drive.

Friday 13th

Aliases: Friday The 13th COM, South African, Virus B

Type: Non-Resident .COM Infector

Origin: South Africa; November 1987   **Variants**: 7

Overview: The original Friday 13th COM virus first appeared in South Africa in 1987. Unlike the Jerusalem (Friday 13th) viruses, this virus is not memory resident, nor does it hook any interrupts.

Method of infection: The virus is usually transmitted by booting a computer with an infected disk.

Symptoms: This virus only infects .COM files, but not the COMMAND.COM. A .COM file will only be infected once. The file, after infection, will be less than 64K in length.

Damage: When an infected file is executed, the virus looks for two other .COM files on the C: drive and one on the A: drive. If found, they are infected.

This virus is very fast, and the only indication of propagation occurring is the access light being on for the A: drive, if the current default is drive C:.

Green Caterpillar

Aliases: 1575, 1577, 1591

Type: Resident .COM and .EXE Infector

Origin: Canada; January 1991   **Variants**: 4

Overview: Green Caterpillar is a memory resident virus that infects both .COM and .EXE files, including the COMMAND.COM.

Method of infection: The virus becomes memory resident when the first program infected with the virus is executed. The COMMAND.COM will also be infected at this time.

Symptoms: Infected files will have their file date and time in the DOS directory updated to the system date and time when the infection occurred. Their file lengths will also show an increase of between 1,577 and 1,591 bytes.

A 'green caterpillar' may appear on your screen and DIR commands appear sluggish.

Damage: This virus will infect one .COM and one .EXE program on the current drive whenever a DOS DIR or COPY command is executed. Green Caterpillar does not spread when programs are executed.

Jerusalem

Aliases: PLO, Israeli, Friday 13th, Russian, 1813(COM), 1808(EXE), Arab Star, Black Box, Black Window, Hebrew University

Type: Resident Generic File Infector

Origin: Italy; October 1987   **Variants**: 41

Overview: Jerusalem is a memory resident virus that infects .COM, .EXE, .SYS, .BIN, .PIF, and overlay files when they are executed. .EXE files may be re-infected by the virus each time they are executed due to a bug in the viral code. The virus has been altered many times, and many other viruses have been based on its code.

Method of infection: The virus is usually transmitted by booting a computer with an infected disk.

The first time a program infected with the Jerusalem virus is executed, the virus will install itself memory resident as a low system memory TSR of 1,792 bytes. Interrupts 08 and 21 will be hooked by the Jerusalem virus in memory.

Symptoms: Once Jerusalem is memory resident, it will infect programs other than COMMAND.COM when they are executed. .COM files will increase in size by 1,813 bytes with the virus located at the beginning of the infected file. .EXE files will increase in size by 1,808 to 1,822 bytes with the virus located at the end of the infected file. Each time an .EXE file becomes re-infected, an additional 1,808 bytes will be added to the file size. Infected files will have no change to their date and time.

Approximately 30 minutes after execution of an infected file, the system's performance will deteriorate by a factor of 10. Some Jerusalem virus variants will have a black window or black box appear on the lower left side of the screen which will scroll with the screen.

Damage: Jerusalem activates after it becomes memory resident on Friday the 13ths. At that time, it will delete any program the user attempts to execute.

Joshi

Aliases: Happy Birthday Joshi, Stealth Virus

Type: Resident Boot Sector/Master Boot Sector Infector

Origin: India; June 1990   **Variants**: 1

Overview: When the virus was isolated in India, it was reported to be widespread in India as well as portions of the continent of Africa. Joshi is a memory resident boot sector infector of diskettes and the hard disk master boot sector (partition table).

Joshi has some similarities to two other boot sector infectors. Like the Stoned virus, Joshi infects the master boot sector of hard disks. Similar to the Brain virus's method of redirecting all attempts to read the boot sector to the original boot sector, Joshi does this with the master boot sector.

Method of infection: The virus becomes memory resident when the system is booted with an infected disk.

Symptoms: Joshi takes up approximately 6K of system memory. Infected systems will show that total system memory is 6K less than is installed when CHKDSK is run.

Joshi activates on January 5th. At that time, the virus will hang the system while displaying the message "type Happy Birthday Joshi". If the user types "Happy Birthday Joshi", the system will again be usable.

Damage: Systems infected with Joshi may experience problems when attempting to access programs or data files on write-protected diskettes.

Michelangelo

Aliases: None

Type: Resident Floppy Boot Sector/Master Boot Sector Infector

Origin: Sweden or the Netherlands; April 1991
Variants: 0

Overview: Michelangelo is a memory resident infector of diskette boot sectors and the hard disk master boot sector (partition table). It is roughly based on the Stoned virus, though it is very different in its behavior.

Method of infection: The virus becomes memory resident when the system is booted with an infected disk. Even if the boot is not successful, Michelangelo will still become memory resident.

Symptoms: Total system and available free memory, as measured by the CHKDSK command, will typically decrease by 2,048 bytes.

Damage: Once Michelangelo is memory resident, it will infect diskette boot sectors as they are accessed. It will also infect the hard disk master boot sector when the user attempts to access a file on the hard disk.

When Michelangelo infects a diskette, it moves the original boot sector to a different location. Entries in the overwritten sector will be lost.

Similarly, when Michelangelo infects the system hard disk, it moves the master boot sector to a different location on the hard disk.

Michelangelo activates on March 6, at which time it will format the system hard disk by overwriting it with random characters from system memory.

Monkey

Aliases: Empire, Monkey.A

Type: Floppy boot sector and Master Boot Record infector

Origin: 1992, Canada   **Variants**: 2

Overview: A very infectious and increasingly common virus, Monkey is a full stealth virus in that in encrypts both itself, the Master Boot Record and both copies of the partition table.

Method of infection: Once resident, Monkey will infect any floppy accessed in the A: or B: drive.

Symptoms: CHKDSK will report conventional memory reduction of 1,024 bytes, e.g. total bytes on 640Kb computer will show 654,336 bytes.

Damage: Various sectors of hard drive may be randomly encrypted.

If user boots from a clean floppy, drive C: will "disappear," returning "Invalid drive specification" message when you attempt to access it. C: becomes visible if you boot with infected floppy or boot from infected C: drive.

NoInt

Aliases: Bloomington, LastDirSect, Stoned III

Type: Resident Boot Sector and Master Boot Sector Infector

Origin: Canada; June 1991   **Variants**: 1

Overview: NoInt is a stealth variant of the Stoned virus. Like Stoned, it infects diskette boot sectors as well as the hard disk master boot sector (partition table).

Method of infection: The first time the system is booted from a diskette infected with the NoInt virus, the virus will become memory resident at the top of system memory, but below the 640K DOS boundary.

Symptoms: Infected systems will take longer than normal to perform disk accesses or system boots. High density infected diskettes will often get a "Disk boot failure" when you try to boot from them.

Damage: Once the virus is in memory, it will infect diskettes as they are accessed on the system. When NoInt infects a diskette, it moves the original boot to a different location. Directory entries may be lost.

One Half

Aliases: Freelove, One_Half

Type: COM file, EXE file and Master Boot Record infector

Origin: 1994, England   **Variants**: 2

Overview: One Half loads in high memory and disguises itself well. Available memory will not be reduced, and when resident it hides 3577 byte size increase it creates in COM and EXE files.

Method of infection: When an infected file is first run, the virus seeks to infect the Master Boot Record. Because it does not infect the floppy boot record, One Half spreads when infected files are copied.

Symptoms: Very few. CHKDSK will not report any errors. However, if CHKDSK is renamed and run with its new name, it will report "Allocation error, size adjusted" when virus is resident.

Damage: When infecting a COM file, the virus will replace the first three bytes of the file with code that makes a jump to itself. It will then append itself to the file.

When infecting an EXE file, the virus places itself as the first bytes in the file.

In all cases, the infection is fully encrypted.

Stoned

Aliases: 1991 Boot, Donald Duck, Hawaii, Marijuana, New Zealand, Rostov, San Diego, Sex Revolution, Smithsonian, Stoned II, Stoned-16, Stoned-AT Love, Stoned-Collor, Stoned-Mexican, Stoned Mutation

Type: Resident Boot Sector and Master Boot Sector Infector

Origin: New Zealand; February 1988   **Variants**: 21

Overview: The original virus only infected 360K 5.25" diskettes, doing no overt damage. That virus is now extinct, and all known variants of the virus can infect the hard disk master boot sector (partition table) as well as damaging directory or File Allocation Table (FAT) information. Most variants of this virus are similar. Usually the only difference is in the text of the message that the virus displays when the computer boots.

Method of infection: The virus is usually transmitted by booting a computer with an infected disk.

Stoned installs itself into the top 2K of memory. The interrupt 12 return will be moved. If the system boot was from a diskette, the virus will also attempt to infect the hard disk master boot sector, if it was not previously infected.

Symptoms: Upon system bootup, the Stoned virus may display a message. The message is displayed more or less on a random basis. The most common text for the message is "Your computer is now stoned" or "Your PC is now Stoned!". The CHKDSK command will indicate that the computer system has 2K less total memory than what is installed.

Damage: Once Stoned is memory resident, it will infect diskettes as they are accessed on the system. When Stoned infects a diskette, it moves the original boot sector to a different address and then copies itself to the original boot sector location. Directory entries may be lost and the disk's FAT may be corrupted.

Similarly, when Stoned infects the system hard disk, it moves the original master boot sector to a different address and then copies itself to the original boot sector location. If the hard disk was formatted with software which starts the boot sector, FAT, or disk directory right after the master boot sector, the hard disk may be corrupted as well.

Telecom

Aliases: Telefonica, Telecom File, Spanish Telecom-2

Type: Resident .COM Infector

Origin: Spain; June 1991   **Variants**: 0

Overview: Telecom carries a variant of the Anti-Tel virus which it will install on the hard disk master boot sector. The Anti-Tel virus is a destructive memory resident infector of the hard disk master boot sector and the diskette boot sector.

Method of infection: The virus becomes memory resident when a program infected with the virus is executed. Once Telecom is memory resident, it infects the hard disk master boot sector and will infect .COM programs larger than approximately 1K in size when they are executed.

Symptoms: The CHKDSK command will indicate the system has 3,984 bytes less memory than what is installed. Infected . COM programs increase in size by 3,700 bytes, though the file length increase cannot be seen in the disk directory listing because the virus hides it. The virus also changes the file's date in the directory by adding 100 to the year, though the virus hides it from the directory listing as well.

Damage: After 400 system boots from an infected disk, the virus will overwrite the system hard drives.

Tequila

Aliases: Stealth

Type: Resident .EXE and Master Boot Sector Infector

Origin: Switzerland; April 1991   **Variants**: 0

Overview: Tequila is a memory resident master boot sector (partition table) and .EXE file infector. It uses a complex encryption method and garbling to avoid detection.

Method of infection: When a program infected with Tequila is executed, the virus will modify the hard disk master boot sector, if it is not already infected. The virus also copies itself to the last six sectors of the system hard disk.

When the workstation is later rebooted from the system hard disk, Tequila will become memory resident. Once Tequila is memory resident, it infects .EXE files when they are executed.

Symptoms: The CHKDSK command will indicate the system has 3,072 bytes less memory than what is installed. Infected . EXE programs increase in size by 2,468 bytes, though the file length increase cannot be seen in the disk directory listing because the virus hides it.

Tequila activates four months after the initial date of infection. At this time, and every month thereafter, the virus will display a graphic and the following message: "Execute: mov ax, FE03 / int 21. Key to go on!".

Damage: The CHKDSK command will detect file allocation errors when the virus is memory resident. If CHKDSK is run with the /F option, program corruption may occur.

Yankee Doodle

Aliases: TP44VIR, Five O'clock Virus

Type: Resident .COM and .EXE Infector

Origin: Bulgaria; September 1989   **Variants**: 15

Overview: Yankee Doodle is a memory resident virus that infects both .COM and .EXE files, excluding the COMMAND.COM.

Some variants of the Yankee Doodle virus will seek out and modify Ping Pong viruses, changing them so they self-destruct after 100 infections.

Method of infection: The virus becomes memory resident when the system is booted with an infected disk.

Symptoms: After installing itself memory resident, it will play Yankee Doodle on the system speaker at 17:00. Infected programs will be increased in length by 2,899 bytes.

Damage: Other than being disruptive by playing Yankee Doodle, this virus currently does nothing else harmful besides infecting files.

B

GETBBS.NLM

GETBBS.NLM will automatically call Cheyenne's bulletin board and retrieve the latest virus signature files for you.

In this chapter, you will learn:

GETBBS Basics

What is GETBBS?

GETBBS is an NLM that automatically calls Cheyenne Software's bulletin board at regular intervals and retrieves the latest virus signature files.

If you normally dial internationally to reach Cheyenne's BBS, note that a local number may now be available for you. Please contact your local Cheyenne support number for information.

GETBBS and InocuLAN keep your system up-to-date

Part of the process of safeguarding your network against viruses involves keeping your InocuLAN virus signature files up-to-date. As new computer viruses are discovered, Cheyenne Software updates InocuLAN's virus signature files and makes them available through Cheyenne's bulletin board (they are also available on CompuServe).

With GETBBS, you do not have to worry about getting the latest virus signature files. GETBBS will do it all for you. And, once the files have been retrieved, InocuLAN will automatically update all of your member servers and workstations. Refer to "Keeping your InocuLAN system up-to-date" in Chapter 3 for more information.

What do you have to do to use GETBBS?

You must load GETBBS on your file server and configure it for your modem in order to use it. (GETBBS was installed when you installed the InocuLAN Server.)

NOTE: You must also have an external modem with
AIOCOMX.NLM loaded in order for GETBBS to be able
to call Cheyenne Software's bulletin board. If this server
has a modem that is used by Alert (the notification
system used by InocuLAN), the modem will be shared
between GETBBS and Alert. You do not need a
separate modem for GETBBS.

Loading GETBBS

In order to configure and use GETBBS, you must load it on your file server.

To load GETBBS:

1. Type **Load GETBBS** at the file server console.

   InocuLAN must be loaded before GETBBS.NLM can be loaded.

   The main menu of GETBBS will appear:

This section of the screen shows the current status of GETBBS.

This section lists the options that are available. (You will only see the *Port Configuration* option when AIOCOMX.NLM is loaded.)

```
┌─────────────────────────────────────────────────────────┐
│                                                         │
│  ┌───────────────────────────────────────────────────┐  │
│  │              GetBBS Status Window                 │  │
│  ├───────────────────────────────────────────────────┤  │
│  │                                                   │  │
│  │                                                   │  │
│  │                                                   │  │
│  │                                                   │  │
│  └───────────────────────────────────────────────────┘  │
│                                                         │
│                  ┌─────────────────────┐                │
│                  │    GetBBS Menu      │                │
│                  ├─────────────────────┤                │
│                  │ Status              │                │
│                  │ Configuration       │                │
│                  │ Port Configuration  │                │
│                  │ Unload              │                │
│                  └─────────────────────┘                │
│                                                         │
│    <F1>:Help   <Enter>:Select  ↑↓ <PgUp> <PgDn>        │
└─────────────────────────────────────────────────────────┘
```
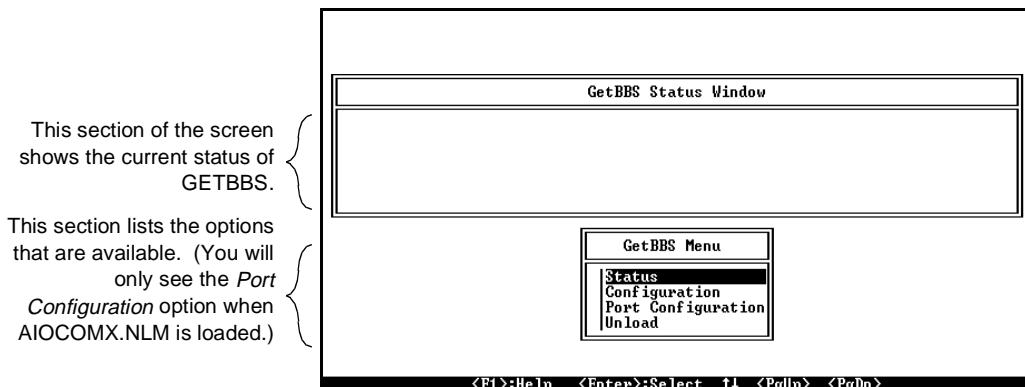
A brief description of each menu option appears below. Detailed information can be found in the next few sections.

Status   This option allows you to view a log containing the status of GETBBS. While the current status is displayed on the main menu, this log contains a historical status listing.

Configuration   This option allows you to set up modem information. It also displays, and lets you modify,

how often GETBBS should call Cheyenne Software's bulletin board.

Port Configuration

This option displays a menu that offers several modem options.

Unload

This option unloads GETBBS. You can also enter UNLOAD GETBBS at the server console.

Configuring GETBBS

Most of the configuration is preset for you. You can change some of the information, if necessary.

To configure GETBBS:

1. Select Configuration from the main menu.

2. Enter information on the Configuration screen.

```
                    Default Configuration Options
  BBS User First Name: InocuLAN          Last Name: Signature
  Cheyenne's BBS Number: 15164843445            Password: Update
  Next Call is on Date: 8 /11/94   Time: 4 :46
  Notify InocuLAN NLM: Yes
  _____
  Scheduling:

  Interval between update calls: 1 Month(s)  0 Day(s)
  If call successful, next time to start dialing: 4 :46
  If call unsuccessful, repeat every 5 Minute(s)
  If unsuccessful in 12 attempts, reschedule to next 1 Day(s)

  _____
  Equipment:
  Modem Speed: 1200  bps   Connection Delay: ,,,
```

BBS User First Name, Last

These fields come preset with the information needed for GETBBS to log in to Cheyenne Software's bulletin board. Do NOT change this information unless you are sure it has changed.

Cheyenne's BBS Number	This field is preset with Cheyenne's BBS number. You may need to modify this number if, for example, your phone system requires you to dial a 9 in order to get an outside line.
Password	This field comes preset with the password needed for GETBBS to log in to Cheyenne Software's bulletin board. Do NOT change this password unless you are sure it has changed.
Next Call is on:	The defaults in this field are based on the date and time you first load GETBBS. The date is one month from the date GETBBS was first loaded. The time is 4:00 a.m. plus the number of minutes after the hour when GETBBS was loaded. For example, if you load GETBBS at 9:15, the time for the next call will be 4:15 a.m. (4:00 plus 15 minutes). This is done to spread out the number of calls coming into Cheyenne Software's bulletin board at any one time.
Notify InocuLAN NLM	This field is preset to notify the InocuLAN NLM when files are retrieved.
Interval between update calls	This field tells you how often GETBBS will call Cheyenne Software's bulletin board.
If call successful, next time to start dialing	This field tells you the time GETBBS will call the bulletin board, the next time it is scheduled to call.
If call unsuccessful, repeat every n minutes	This field tells you how often GETBBS will retry the call, if the call is unsuccessful. The call will be retried for the number of times specified in the next field.

If unsuccessful in n attempts, reschedule to next n Days	This field tells you how many times GETBBS will retry the call before rescheduling it for another day. You determine how many days to wait before rescheduling.
Modem Speed	Indicate the baud rate used by your modem.
Connection Delay	Enter a comma for each delay you want to wait between the time the modem finishes dialing and GETBBS is ready to log in. Typically, a comma represents a one second pause. However, this may vary by brand of modem. Check your modem guide for more information.

Port Configuration

The menu option only appears if AIOCOMX is loaded and a comm port is detected on the server.

When you select *Port Configuration*, the following menu appears:

```
┌─────────────────────────┐
│     Port Configuration  │
├─────────────────────────┤
│ Attach Modem To Port    │
│ Detach Modem From Port  │
│ Reset Modem             │
└─────────────────────────┘
```
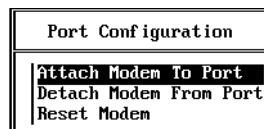
Attach Modem To Port	You should use this option in order to tell GETBBS which port to use. You would need to do this if GETBBS does not report that a modem is attached. This might happen if the modem was off when GETBBS was loaded.

To use this option:

1. Select Attach Modem To Port

2. Select a port from the window that appears.

```
┌─────────────────────────┐
│      Select Port        │
├─────────────────────────┤
│ Board #0/Port #0        │
│                         │
│                         │
│                         │
└─────────────────────────┘
```
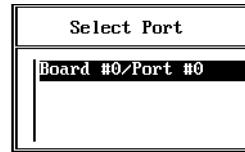
Detach Modem From Port

You could use this option if you wanted to detach a modem because it was not working properly.

To use this option:

1. Select Detach Modem From Port

2. Select a port from the window that appears.

Reset Modem

Your modem is automatically reset when GETBBS is loaded. You could use this option if you had a modem problem, such as a communication that did not end properly and locked your modem.

To use this option:

1. Select Reset Modem

C

INSTALLING INOCULAN MANAGER ON THE CLIENT DESKTOP

Installing the complete program provides LAN users with a strong frontline defense against infection.

Why Install Inoculan Manager	At the first login, the Real Time Monitor is installed automatically. By taking the next steps and installing the full functionality of InocuLAN on every desktop in your enterprise, you provide a stronger frontline defense against infection.
Installing IocuLAN Manager on Windows Desktops	After AVUPDATE installs the Real Time Monitor, do the following to complete the installation:

On the Windows95 or 3.x desktop, open Start/RUN or File/ RUN

> Verify that following path is specified:
>
> F:\MW\INOCULAN\DOWNLOADS\95\Disk1 \Setup.exe (if not, enter or browse to the correct directory)
>
> Click Enter or press Return to begin installation.

Installing InocuLAN on Macintosh Desktops	At the time of this writing, there was to be a radio button to create an InocuLAN for Macintosh installation disk on the startup screen of the ManageWise CD. For more information, see Chapter 10 and the product Readme file.
Windows NT	Included on the ManageWise CD is InocuLAN for Windows NT. This is a stand-alone implementation. For further information, consult Chapter 1 of the AVUPDATE Manual or the InocuLAN AntiVirus Guide.

I N D E X